GE Hitachi Nuclear Energy

NEDO-34197

Revision A

January 2025

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

BWRX-300 UK Generic Design Assessment (GDA) Chapter 25 – Security

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

NEDO-34197 Revision A

INFORMATION NOTICE

This document does not contain proprietary information and carries the notations “US Protective Marking: Non-Proprietary Information” and “UK Protective Marking: Not Protectively Marked.”

IMPORTANT NOTICE REGARDING CONTENTS OF THIS REPORT

Please Read Carefully

The design, engineering, and other information contained in this document is furnished for the purpose of obtaining the applicable Nuclear Regulatory Authority review and determination of acceptability for use for the BWRX-300 design and licensing basis information contained herein. The only undertakings of GEH with respect to information in this document are contained in the contracts between GEH and its customers or participating utilities, and nothing contained in this document shall be construed as changing those contracts. The use of this information by anyone for any purpose other than that for which it is intended is not authorized; and with respect to any unauthorized use, no representation or warranty is provided, nor any assumption of liability is to be inferred as to the completeness, accuracy, or usefulness of the information contained in this document. Furnishing this document does not convey any license, express or implied, to use any patented invention or any proprietary information of GEH, its customers or other third parties disclosed herein or any right to publish the document without prior written permission of GEH, its customers or other third parties.

UK SENSITIVE NUCLEAR INFORMATION AND US EXPORT CONTROL INFORMATION

This document does not contain any UK Sensitive Nuclear Information (SNI) subject to protection from public disclosure as described in the Nuclear Industries Security Regulations (NISR) 2003, does not contain UK Export Controlled Information (ECI), and does not contain US Export Controlled Information (ECI) subject to the export control laws and regulations of the United States, including 10 CFR Part 810.

EXECUTIVE SUMMARY

The BWRX-300 UK Generic Design Assessment (GDA) Preliminary Safety Report Chapter 25 presents at a high-level how the BWRX-300 utilizes protective and cyber security to provide a robust security informed design for the protection against malevolent actions, intended to cause radiological releases that could impact the health and safety of the public.

Claims and arguments relevant to GDA step 2 objectives and scope are summarized in Appendix A, along with a security claims structure. Appendix B provides a Forward Action Plan.

ACRONYMS AND ABBREVIATIONS

Acronym	Explanation
CBSyS	Computer Based Security Systems
CySSP	Cyber Security Plan
D-in-D	Defence-in-Depth
DBT	Design Basis Threat
DCIS	Distributed Control and Information System
DP-SC	Diaphragm Plate Steel-Plate Composite
EZ	Exclusion Zone
FSyP	Fundamental Security Principle
GDA	Generic Design Assessment
GEH	GE Hitachi Nuclear Energy
GSR	Generic Security Report
HFE	Human Factors Engineering
HVM	Hostile Vehicle Mitigation
I&C	Instrumentation and Control
ICS	Isolation Condenser System
IT	Information Technology
KSyPP	Key Security Plan Principle
NISR	Nuclear Industries Security Regulations
NM	Nuclear Material
ONR	Office for Nuclear Regulation
ORM	Other Radioactive Material
PA	Protected Area
PAAB	Protected Area Access Building
PIDS	Perimeter Intrusion Detection System
RB	Reactor Building
SC1	Safety Class 1
SC2	Safety Class 2
SC3	Safety Class 3
SCN	Non-Safety Class
SDLC	Software Development Lifecycle
SNI	Sensitive Nuclear Information
SSCs	Structures, Systems, and Components
SyAPs	Security Assessment Principles
SyBD	Secure-by-Design
TS	Target Set

Acronym	Explanation
TSE	Target Set Element
U.S.	United States
UK	United Kingdom
UPS	Unifying Purpose Statement
VA	Vital Area
VBS	Vehicle Barrier System

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

None.

NEDO-34197 Revision A

REVISION SUMMARY

Revision #	Section Modified	Revision Summary
A	All	Initial Issuance

25. SECURITY

The BWRX-300 GDA Preliminary Safety Report Chapter 25 (Security) presents at a high-level how the BWRX-300 provides a robust security informed design for the protection against malevolent actions, intended to cause unacceptable radiological releases that could impact the health and safety of the public.

This results in the following key fundamental capabilities remaining available after malevolent actions.

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

Further detailed information regarding the protective security design can be found within 006N6248 BWRX-300 Security Assessment and is referenced throughout PSR Ch. 25 sections to provide a linking guide to the more detailed topic information it contains. The 006N6248 BWRX-300 Security Assessment document provides the detailed information that will enable a future duty holder/licensee to implement the security case.

Detail of the duty holder/licensee arrangements are currently unknown. Therefore, at this stage the scope of this chapter is limited to a summary and guidance of the security philosophies and principles of the BWRX-300 security informed standard design.

Appendix A summarizes the Claims relevant to the UK GDA step 2 objectives and scope.

Appendix B provides a Forward Action Plan.

25.1 Security Summaries

This section provides a general information summary of security features which apply to BWRX-300.

25.1.1 Protective Security

Protective security is provided through a combination of a security organization, including armed personnel, physical barriers, controlled access to the Protected Area (PA), controlled access to vital areas located within the PA, and administrative policies and procedures for screening and monitoring personnel and material allowed access to the site.

All Vital Areas (VA) are located within the PA. With the exception of certain staff workstations, such as the Main Control Room and Central Alarm Station, all vital areas are within the Reactor Building. Much of the vital equipment is within containment which is inaccessible during operation and typically only accessed during refueling intervals and to which access is monitored and controlled. The location of VAs within the Reactor Building provides a second physical site barrier and means of access control.

The Defence-in-Depth (D-in-D) concepts of redundancy and physical separation of redundant systems, as well as simple passive safety systems, further support the physical security of the plant in that multiple vital Structures, Systems, and Components (SSCs) must be compromised to realize effective radiological sabotage.

All vital systems and components are housed within robust steel-concrete composite structures that can only be accessed through a minimal number of normally locked access points that are controlled and monitored by the site security system. Many of the components of vital systems are located below site grade, thereby minimizing exposure to external threats.

25.1.2 Cyber Security

GEH implements strong cyber security programmes to control the product development lifecycles for all disciplines susceptible to cyber security issues, across both the Computer Based Security Systems (CBSyS) and the Instrumentation and Control (I&C) technology platforms. GEH’s product security program is based on common industry standard frameworks, with the objective to achieve high assurance that unauthorized access to the protection, control, and adjustment systems of the BWRX-300 is prevented.

The GEH cyber security programme is designed to protect the BWRX-300 design and associated standard plant envelope from a cyber-attack or event. GEH initialized this comprehensive programme at the early phases of planning and so allows the licensees to take credit for the cyber security programme and the security features designed into the BWRX-300 systems. BWRX-300 incorporates advanced cyber security principles by leveraging industry standards within the product development, procurement, and deployment lifecycle of the BWRX-300 and its information, communications, and automation systems.

25.2 Site Layout and the Protected Area

The BWRX-300 site consists of an Exclusion Zone (EZ) where public access is restricted; within which is the PA measuring approximately 200 meters by 160 meters, which is a zone further restricted to employees and approved visitors. The PA boundary consists of a physical barrier with an isolation zone on either side of that barrier and detection systems to monitor and assess for persons attempting to cross the barrier.

The PA surrounds all VAs and serves to limit access to important SSC to only persons who have been properly vetted and have a need for access. A visitor access programme to enact due-diligence and order of entry rules, will be implemented to allow unvetted persons who have a valid need to enter the site to be escorted by qualified personnel.

The PA perimeter consists of a barrier with isolation zones and intrusion monitoring that surrounds all operating structures of the BWRX-300 site. The intrusion detection system alarms to indicate attempted access to the site in locations other than intended and is continuously monitored by qualified staff. Required penetrations of the PA barrier by utilities and other piping are configured to prevent opportunity for ingress, and underground pathways such as storm sewers, culverts, service piping, and cable routing that traverse the PA boundary are made inaccessible at or near the point they cross under the PA.

The PA perimeter consists of multiple systems which fulfil several security purposes:

- A PA fence serves as a personnel access barrier, except through designated portals.
- A Protected Area Access Building (PAAB) provides for authorized personnel access into the PA.
- Cameras and perimeter lighting provide for surveillance of the PA fence and isolation zone.
- An isolation zone provides a restricted area on either side of the PA fence to enhance detection of attempts to improperly enter the site or to tamper with the barrier. Presence in this restricted area alerts security to enhanced observation and response to the presence.
- A Perimeter Intrusion Detection System (PIDS) electronically monitors the PA fence and exterior isolation zone. The PIDS alarms to alert the security staff to a presence and displays camera surveillance of the area.
- A Vehicle Barrier System (VBS) serves to prevent vehicle access, except through designated portals, and will qualify as a Hostile Vehicle Mitigation (HVM) barrier. A Sally Port serves as a search area and ingress/egress portal for vehicles.
- Civil utilities potentially requiring repair or maintenance by non-employees in the PA will be minimized.
- A secondary egress portal is provided in the PA boundary for emergency exit in the event the PAAB ingress/egress portal is unavailable due to emergency situations.

The ingress/egress into the PA is through the PAAB, where identity and access rights are determined before allowing entry. All personnel, packages, and vehicles entering the PA are searched through electronic or hands-on methods. Bulk deliveries and consumable supplies are delivered outside the PA to prevent introduction of contraband into the PA.

A vehicle sally port is provided near the PAAB, which provides vehicle access through the PA barrier. The sally port is a dual barrier enclosure where the outer barrier may be opened to allow a vehicle to enter, the outer barrier closed, the vehicle searched, and then the inner barrier opened to allow the vehicle to enter the PA. This method provides for a continuous PA barrier even when admitting or releasing vehicles.

Further details relating to the BWRX-300 site characteristics and key plant systems can be found within Chaps 4 & 5 of 006N6248, “BWRX-300 Security Assessment,” (Reference 25-1).

25.3 Design Basis Threat

GEH has developed a single bounding proxy Design Basis Threat (DBT) that establishes a set of credible characteristics, capabilities, and techniques for the theft or sabotage of Nuclear Material (NM) or Other Radioactive Material (ORM), to support the BWRX-300 reactor design to be licensable in multiple countries.

The GEH proxy DBT, to which the BWRX-300 design is subjected, must meet the DBT detailed criteria for all the potential countries of deployment. Use of a bounding DBT by GEH for standard design purposes does not commit licensees to the GEH proxy DBT, as it is recognized that nations will likely require use of their country specific DBT for further detailed design development for deployment and operations.

The goal of the proxy GEH DBT is to create assurance that the country of licensure's DBT is achievable within the standard design, and so a move to the country specific DBT from the bounding GEH proxy DBT for detailed and site-specific design is easily realizable.

The BWRX-300 standard design has undergone systematic, detailed security design reviews to identify potential weaknesses and pathways within the scope of the GEH proxy DBT that could be exploited. This enabled a security informed and improved design that is cognizant of the proxy generic threat. Security design reviews based on a DBT will continue throughout the design finalization, construction, commissioning, and operational processes to ensure a cost-effective yet well protected site.

The BWRX-300 Proxy Design Basis Threat can be found within 006N6248 BWRX-300 Security Assessment: Appendix A, with additional detail in Chap 6, Sect 6.1 (Reference 25-1).

25.4 General Security Design Principles

The BWRX-300 protective security systems are guided by an iterative and ongoing design process that incorporates changes in threat, evolution of identified vulnerabilities, continuous improvement, and advances in standard physical and cyber protection approaches, systems, and technologies.

25.4.1 Defence-in-Depth

Use of D-in-D ensures that the site defence does not rely solely on one component or element to perform a required function. The D-in-D concept employed in the BWRX-300 design relies on concentric integrated, but independent, layers of defence used to deplete resources or delay progress for an adversary for subsequent interdiction or neutralization.

D-in-D also diversifies the equipment locations of alternate methods of performing each function to limit the value of any one location, and utilizing multiple methods of mitigating the effects of equipment damage reduces reliance on any single strategy. Critical security functions include alternate or backup methods and are designed with considerations for failure tolerance.

Diversity in location and methodology is part of the GEH general design approach for the three key safety functions identified in the introduction to this chapter, and includes consideration of structural performance objectives, threat characterization, material properties, general principles of analysis and design, structural acceptance criteria, and design of SSC.

Further detail on the BWRX-300 Design Principles can be found within 006N6248 BWRX-300 Security Assessment: Chap 7, Sect 7.4 and Appendices M and N (Reference 25-1).

25.4.2 Secure-by-Design

The BWRX-300 development included a security informed design approach from the early stages of concept design that uses sound engineering principles to have minimum impact on cost and maximum effect on support to security outcome performance.

GEH used a Secure-by-Design (SyBD) process that involves security vulnerability reviews during plant design in order to resolve proxy DBT and security issues at the most appropriate phases of design work stage. Placement and number of doors, wall thicknesses to optimize resistance to breaching, and equipment placement to facilitate better target set diversity were all achievable as security was integrated at an early design stage.

Continual design reviews against the proxy DBT capabilities during the entire design evolution ensure that emergent issues were, and will continue to be, identified, and addressed as early as possible. The goal of SyBD is to minimize the operational and maintenance costs of security through better utilization of SSC (including diverse locations) to provide a significant deterrent and defensive benefit versus additional reliance on extrinsic security controls and armed personnel response.

Further detail on the BWRX-300 Design Principles can be found within 006N6248 BWRX-300 Security Assessment: Chap 7, Sect 7.4 and Appendices M and N (Reference 25-1).

25.4.3 Holistic Security

GEH adopts a holistic approach to security where each aspect of security (Deter, Detect, Delay, Deny, Respond, Defend, insider threat) builds on and amplifies other aspects as a means to disincentivize the selection of a BWRX-300 reactor as a target; as well as to increase the effectiveness of the defence and time for onsite or offsite armed responders to interdict intruders before damage leading to severe consequences can be caused.

In addition, by ensuring multiple fully redundant, diversely located, safety SSC, that requires long routes over resource intensive and well protected pathways, serves as a deterrent as well as a delay feature and enhances protective and defensive effectiveness.

Security SSC are designed with fault-tolerance in the protective security systems to ensure further effective D-in-D through complementary detection and assessment systems resistant to failures through removal of consequence from any single component failure. Holistic security enables production of an effective and efficient Security solution that thereby reduces overall plant costs.

25.4.4 Defensive Strategy

This approach focuses on protecting the passive plant features and other key reactor components from hostile action by:

- Creating a robust perimeter.
- Analyzing the potential adversary pathways to critical components.
- Determining adversary resources required to execute the path.
- Slowing the adversary movements and depleting the adversaries' resources before the path can be completed.
- Armed engagement as necessary to neutralize threat.

The BWRX-300 design limits the ability of malicious individuals to cause damage to key systems. This, along with the inherent slower accident progression of the BWRX-300 reactor, reduces or eliminates the reliance on immediate onsite armed responders to prevent substantial offsite radiological releases, which allows for longer-term offsite source response for interdiction and neutralization. During the design process, the following design enhancements have been made to improve the ability to defend the site against malevolent acts:

- The number of entrances to the Reactor Building (RB) were minimized while maintaining emergency exits for personnel safety.
- The Isolation Condenser System (ICS) cooling water pools were moved such that they are no longer in contact with external walls where they were vulnerable to draining by external breaching.
- The Spent Fuel Pool was moved such that it is no longer in contact with external walls where it was vulnerable to draining by external breaching.
- The Spent Fuel Pool walls were thickened, and steel clad on both sides of the walls to be substantially more robust against breaching with the proxy DBT allowable quantity of high explosive.
- RB wall construction utilizes Diaphragm Plate Steel-Plate Composite (DP-SC), which has substantially better resistance to explosive breaching.
- ICS piping was redesigned to be inaccessible by routing directly from containment to the ICS heat exchangers in the ICS cooling water pools to eliminate a potential exposure to malevolent action.
- Cable routing for critical systems was diverted, to the extent practical, to route directly into containment and minimize the number of locations available for malevolent actions.
- Key doors and access hatches were upgraded to be substantially more robust against explosive breaching. Security credited doors are designed to be equally robust to the walls in which they are located.
- Large ducts and openings were enhanced to maintain the same robustness to breaching as the walls in which they are located.

- Bulk deliveries and hazardous material deliveries were moved outside the PA to reduce the opportunity for introduction of hidden explosive devices.

A supplemental design philosophy, should depletion of the adversary resources not be fully achievable, is to channel adversaries into a limited number of heavily defended choke points to optimize defender value and reduce the number of armed staff to a minimum whilst ensuring the relevant security outcome is still delivered.

Choke points are created by limiting the number of exterior access points to structures with critical equipment and design of internal passageways with defendability in mind. Armed personnel located in layers at, near, or along these choke points provide a substantial defensive barrier with minimal security personnel.

The security design provides for a strong and resilient defence, predominantly through passive methods, as a means to minimize operation and maintenance costs (e.g., concrete walls, heavy steel doors, and underground facilities). Where active features are used, such as surveillance systems, access control systems, and automatic door closers, the lifetime maintenance and replacement costs are considered in optimizing the overall lifetime cost of power.

Further detail on the BWRX-300 defensive strategy can be found within 006N6248 BWRX-300 Security Assessment: Chap 7 and Appendices C, F, H, and K (Reference 25-1).

25.4.5 Analytical Methods to Support Security Design Assessment

The defensive strategy is a combination of structural design and channeling, to enhance security effectiveness and minimize staffing while maintaining an effective defence.

The structural wall thickness determines the breaching resources, in the form of tools and high explosives, which are required for adversaries to transit a given route. Channeling is best performed by having alternate routes require significantly more time and resources, forcing an adversary to choose to enter at a well-defended portal.

Optimal channeling is achieved when all possible routes converge at a limited number of points. This allows the most effective use of weapons and personnel for defence of these few points.

GEH utilizes computer modelling of potential adversary pathways to determine the resource demands of all possible routes from the perimeter to any combination of locations that represented a target set. By altering the number and location of openings, door characteristics, and wall thicknesses in various areas, effective channeling has been achieved.

Analysis shows which routes are beyond the allowable resources of the proxy DBT and which are not. Further analysis of the data revealed effective channeling locations, for maximum effectiveness.

Further detail on the BWRX-300 Analysis software tools can be found within 006N6248 BWRX-300 Security Assessment: Chap 9 (Reference 25-1). Python code used for analysis is documented in 006N6248 as part of the analysis results within Appendices C and E.

25.4.6 Mitigation Actions

Mitigation Actions are activities which reduce, alter, or eliminate the consequences of an adversary action. If mitigation efforts are available, either before or after the adversary action, then these actions may be included in the target set logic. Mitigation actions are only allowed if it can be shown that the personnel performing the actions can do so without undue risk of injury or death.

25.4.7 Layered Access Requirements

A layered access control strategy is used to limit access to equipment and components based on the equipment's relative significance to the overall protective strategy.

25.4.8 Safety/Security Interface

Safety measures, protective security measures, and cyber security controls are designed and implemented during plant operations in an integrated manner so that they do not compromise one another.

25.4.9 Human Factors Engineering

GEH applies a risk-based Humans Factors methodology to inform the following:

- Operating experience review to determine lessons learned from previous plants of similar designs and technologies.
- Definition of functional requirements and allocation of security functions to automatic (machine), manual (human), or shared actions.
- Security task analysis, task sequencing, and workload analysis to confirm security staffing assumptions and to provide task support requirements to inform the design of human system interfaces and procedures.
- Application of Human Factors design requirements to the security alarm stations and human system interfaces.
- Walkthroughs or dynamic simulation testing to validate staffing levels and efficacy of the design.
- Credit human actions for security, security success criteria, and security testing scenarios.
- Facility layout
- Conflicts of interest

Further detail on the BWRX-300 Human Factors Engineering (HFE) Plan can be found within 006N6248 BWRX-300 Security Assessment: Chap 8 and Appendix I (Reference 25-1).

25.5 Vital Areas and Target Sets

25.5.1 Vital Areas

Areas containing NM or ORM inventory and/or SSC that are determined to be especially important to plant nuclear safety or in preventing radiological release, that are sabotaged, and would be capable of causing an unacceptable radiological consequence, are designated as VAs. In addition, locations whose loss through sabotage would significantly impact the protective security or cyber security response to a threat are also included as VAs.

The methodology regarding determination of VAs is contained in Appendix D of 006N6248 BWRX-300 Security Assessment: (Reference 25-1).

25.5.2 List of Vital Areas

The list of VAs is protected information and is contained in 006N6248 BWRX-300 Security Assessment: Appendix D (Reference 25-1).

25.5.3 Target Set Identification Methodology

BWRX-300 Target Sets (TS), and subsequently the VAs that contain them, are created using the probabilistic risk assessment, design-basis events, beyond-design-basis events (of both natural and man-made sources), emergency procedures, severe accident analysis, and other analyses of potential core damage sequences.

This process enables identification and development of Target Set Elements (TSEs) whose loss of proper function would lead to unacceptable levels of offsite release of radioactive material. TSEs are the components in those critical systems that, if damaged or destroyed, would cause the loss of function of that system.

TS are logical groupings of TSE components that, if all were made inoperable for a defined period by adversaries, the inoperability would inevitably lead to substantial and/or unacceptably large offsite doses. Only events and components that contribute integrally to the final conclusion are included in the target set.

Logic may be arranged in either a failure set logic (Boolean logic, which if analyzes True, confirms an excessive radiological release) or a success set logic (Boolean logic, which if analyzes True confirms excessive offsite releases are prevented). The BWRX-300 design uses a success set version of target set logic. This logic is more aligned with methodologies for operating procedures, security protective logic, and emergency response prioritization.

The TS and TSE components are then converted to physical locations within the plant. Using physical locations instead of components in the logic better aligns with the defensive logic of security and makes the target set more effective as a training tool. It also reveals co-dependencies between multiple target sets on a particular location or area, which would indicate a need for enhanced defensive measures.

VAs are then developed from these physical locations. Several smaller VAs in a general vicinity may be grouped together into a larger VA to simplify access control.

Further detail on VAs, TS, and TSE and the methodologies to identify and categorize them is contained in 006N6248 BWRX-300 Security Assessment: Chap 6 and Appendices D and E (Reference 25-1).

25.5.4 Vital Areas and Defensive Strategy

The site defensive strategy is to prevent or delay access to VAs so that onsite or offsite defensive forces have sufficient time to interdict adversaries prior to access or create sufficient damage to plant equipment that could result in unacceptable offsite radiological releases.

In evaluating defensive engagements, inadvertent damage to vital equipment in the area by defensive forces is considered.

Further detail on the BWRX-300 defensive strategy can be found within 006N6248 BWRX-300 Security Assessment: Chap 7 and Appendices H and K (Reference 25-1).

25.5.5 Vital Areas and Insider Mitigation

The plant security design considers the threat from an insider that is assisting the malevolent forces. Whether due to coercion or affiliation, the possibility for insider physical or cyber sabotage of critical equipment must be addressed. To reduce the opportunity for sabotage, access to VAs, and therefore TS and TSEs, is limited to those with a need to work in VAs, having had sufficient background and security vetting checks. In addition, behavioural observation through internal surveillance in high significance areas and information and control systems restrictions provide a further defence against tampering.

Further detail on the BWRX-300 insider threat analysis can be found within 006N6248 BWRX-300 Security Assessment: Chap 6, Sect 6.6.3 (Reference 25-1).

25.6 Security Design and Assessment Standards and Guidance

Detail regarding the BWRX-300 standard design code, standards, and guidance can be found within 006N6248 BWRX-300 Security Assessment: Chap 3 (Reference 25-1).

25.7 Cyber Security

Cyber security has become a critical consideration with the design and usage of digital control systems. These systems, including Computer Based Systems Important to Nuclear Safety, Computer Based Systems Essential to Safe Operations, and Computer-Based Security systems computers, including network communication systems are adequately protected against cyber-attacks up to and including threat categorization within DBTs, through application of SyBD and D-in-D principles in a cyber security defensive architecture, which extends over the entire equipment lifecycle.

25.7.1 Cyber Security Programme Plan

The 006N6731, “BWRX-300 Plant Cyber Security Plan (CySSP),” (Reference 25-2) describes the methodology and process to identify nuclear safety critical systems including systems located in VAs, as well as the application of the cyber risk assessment methodology against identified systems to apply appropriate mitigating controls. It also describes the integration of requirements from standards and regulations into the design approach of systems engineering and the software development process.

The CySSP is designed to protect the BWRX-300 digital I&C systems and associated standard plant envelope from a cyber-attack or event. GEH initialized the CySSP at the early phases of planning, to steer the design of critical systems to ensure D-in-D by implementing proportionate controls to reduce cyber risks to as low as practicable. The CySSP is a conservative set of standards that are consistent with both North American and international standards.

The BWRX-300 CySSP incorporates cyber security principles and recognized good practice throughout the development lifecycle while ensuring regulatory compliance. The objective of the CySSP is to achieve a high assurance that unauthorized access to the protection, control, and adjustment systems of the BWRX-300 is prevented. This high assurance is achieved by performing a risk assessment, implementing cyber security controls, and maintaining these cyber security controls throughout the system lifecycle. By design, the CySSP provides a framework to incorporate the most appropriate standards and processes at the time the plan is initiated. The framework is based on “NIST Cyber Security Framework,” (Reference 25-8) with the main steps of the framework being the following.

- Identify cyber assets and classify them using a graded approach.
- Implement cyber security controls to protect critical essential assets from cyber security events.
- Apply and maintain a defensive cyber security architecture protective strategy to ensure the capability to identify, protect, detect, respond, and recover from cyber events.
- Ensure that the functions of protected assets identified are not adversely impacted due to cyber events.

The wider plan has been designed to align with required cyber security program elements from NRC, CNSC, and IEC to create a global cyber security program for digital I&C, cyber security guidance, recognized best practices, and regulatory requirements continue to evolve over time, and GEH is committed to regulatory requirements at the time of licensing submittal.

Furthermore, 007N8080, “Cyber Security Controls for the Software Development Lifecycle (SDLC),” (Reference 25-5) describes the process for managing cyber security risk and reducing the number of security vulnerabilities in each phase of the SDLC.

25.7.2 Cyber Security Risk Assessment

007N2681, “BWRX-300 System Cyber Security Assessment Process,” (Reference 25-3) describes the process to identify cyber critical assets which includes nuclear safety systems which may be located within vital areas or could impact nuclear safety due to a loss of availability or integrity. The process also describes how to classify the safety and security impact of digital assets and ensure relevant controls and security outcomes are implemented.

25.7.3 Computer Based Security Systems

Further details on the BWRX-300 Security Computer System Cyber Security Plan can be found within 006N6248 BWRX-300 Security Assessment: Appendix G (Reference 25-1).

The plant design includes dedicated locations for hosting the CBSyS with consideration given for required protective and personnel security controls. These locations are described within 006N6248 BWRX-300 Security Assessment: Appendix G (Reference 25-1).

Cyber security mitigations will be implemented during the detailed and site-specific design phases. The Cyber Security Programme Plan implementation will be considered at the time of system design to ensure relevant risk assessments and controls are implemented.

25.7.4 Plant Instrumentation and Controls

The defensive cyber security architecture to deliver D-in-D of the I&C network architecture is based on recognized good practice from IEC 61513:2011, “Nuclear Power Plants – Instrumentation and Control Important to Safety – General Requirements for Systems,” (Reference 25-9) and IEC 62859, “Nuclear Power Plants – Instrumentation and Control Systems – Requirements for Coordinating Safety and Cybersecurity,” (Reference 25-10). Establishing cyber security boundaries on groups of systems with similar safety and security significance provides D-in-D, with the aim to delay and disrupt unauthorized lateral movement across the network and provide the ability to detect suspicious activities. In addition, utilization of unidirectional communication controls further reduces opportunity of unauthorized lateral movement. Further detail on defensive layers and defensive security measures to detect, prevent, delay, mitigate, and recover from cyber-attacks can be found within 007N5118, “BWRX-300 Defensive Cyber Security Architecture,” (Reference 25-4).

The cyber security methodology to restrict communication flows between the security levels is based upon the Biba-integrity model and ensures that communication flows unidirectionally from the highest significance security level to the lowest using fail-secure, deterministic communication pathways.

This integrity model takes a nuclear centric approach of protecting cyber assets by prioritizing the integrity of systems important to safety over all other systems. The separation of networks into Security Levels allows for the enhanced capability to detect, prevent, delay, mitigate, and recover from cyber-attacks.

Security Levels and Security Zones play two different roles in the Defensive Cyber Security Architecture:

- Security Levels are a high-level grouping of systems based on their common cyber security control requirements and importance to plant protection.
- Security Zones are a more granular segmentation of systems and their networks, and the tightly coupled communications that are essential for the system to perform its critical functions.
    - Security Zones should be self-contained and able to function independently and locally even if the surrounding Security Zones are offline.

- Security Zones have defined boundaries.
- Security Zones, their zone boundaries, and required network communications are defined, documented, and maintained for every control system in that system's System Design Description

The Security Levels are distinct from one another and are defined as follows:

Level 4:

- Cyber essential assets of a high safety significance, including Safety Class 1 (SC1), are allocated to Level 4 and are protected from all lower levels.
- Only unidirectional communications from Level 4 to Level 3 are allowed. This unidirectional communication is enforced with a hardware data diode to ensure the security boundary of Level 4 is isolated from Level 3.
- Level 4 contains the safety network, a network for safety information systems.

Level 3:

- CEAs with moderate or low security significance, including Safety Class 2 (SC2), Safety Class 3 (SC3), and Non-Safety Class (SCN) systems, reside in Level 3.
- Level 3 contains the plant network, which includes the Distributed Control and Information System (DCIS) and all other cyber assets that are not high safety significance.
- Only unidirectional communications from Level 3 to Level 2 is permitted. This unidirectional communication is enforced with a data diode to ensure the security boundary of Level 3 is isolated from Level 2.

Level 2:

- The business network is contained in Level 2. The business network is a shared demilitarized zone between Information Technology (IT) and operational technology. This network is considered untrusted and is managed by the licensee and their IT department.

Level 1:

- Level 1 is the enterprise or corporate IT network. This network is managed by the licensee's IT department and is outside of the scope of this document.
- It may be situationally relevant that personnel inside of the protected area require access to enterprise network resources for business related tasks. These resources are required to be air gapped from Levels 4 through Level 3.

Level 0:

- Level 0 is the internet or cloud networks.
- Direct communications from any systems residing within Level 4 or Level 3 are strictly prohibited by the use of major enforcement boundary devices.

25.7.5 Cyber Security Codes and Standards

To ensure that the cyber protections are effective in providing a secure operational environment with defensive features but do not interfere with the functions or performance of the systems, existing codes, standards, and recognized good practices will be incorporated to the extent possible.

Detail regarding the BWRX-300 standard design code, standards, and guidance can be found within the cyber security documents referenced (References 25-2, 25-3, 25-4, 25-5) within Section 25.7, and its subsections, of this Chapter.

25.8 References

25-1 006N6248, “BWRX-300 Security Assessment,” Rev 1.

25-2 006N6731, “BWRX-300 Plant Cyber Security Plan,” Rev 2.

25-3 007N2681, “BWRX-300 System Cyber Security Assessment Process,” Rev B.

25-4 007N5118, “BWRX-300 Defensive Cyber Security Architecture,” Rev B.

25-5 007N8080, “Cyber Security Controls for the Software Development Lifecycle,” Rev A.

25-6 NEDC-34140P, “BWRX-300 UK GDA Safety Case Development Strategy,” GE-Hitachi Nuclear Energy, Americas, LLC.

25-7 “Security Assessment Principles for the Civil Nuclear Industry,” Version 1, Office for Nuclear Regulation, 2022 Edition.

25-8 “NIST Cyber Security Framework,” V1.1, National Institute of Standards and Technology.

25-9 IEC 61513:2011, “Nuclear Power Plants – Instrumentation and Control Important to Safety – General Requirements for Systems,” International Electrotechnical Commission.

25-10 IEC 62859:2016, “Nuclear Power Plants – Instrumentation and Control Systems – Requirements for Coordinating Safety and Cybersecurity,” International Electrotechnical Commission.

APPENDIX A CLAIMS, ARGUMENTS AND EVIDENCE

The CAE approach can be explained as follows:

1. Claims (assertions) are statements that indicate why a facility is safe and secure,
2. Arguments (reasoning) explain the approaches to satisfying the claims,
3. Evidence (facts) supports and forms the basis (justification) of the arguments.

The GDA CAE structure is defined within NEDC-34140P, “BWRX-300 UK GDA Safety Case Development Strategy,” (Reference 25-6) and is a logical breakdown of an overall claim that:

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

This overall claim is broken down into Level 1 claims relating to environment, safety, security, and safeguards, which are then broken down again into Level 2 related sub-claims and then finally into Level 3 sub-claims.

The breakdown of claims relating to the security case are detailed within Table A-1.

Table A-1: Security Claims Structure

<table>
<tr><th colspan="3">Security Level 1 Claim (Unifying Purpose)</th></tr>
<tr><td colspan="3">SyL 1. The nuclear security arrangements of the BWRX-300 shall protect the public and environment from the risks arising from an unacceptable radiological consequence resulting from:
Malicious actions of sabotage of nuclear material, other radioactive material;
And/or of structures, systems, and components maintaining or supporting plant and nuclear safety;
The theft of nuclear material and other radioactive material;
Or through the compromise of Sensitive Nuclear Information (SNI).</td></tr>
<tr><td>SyL1 Note</td><td colspan="2">Tier 1 claim directly links to the Unifying Purpose Statement (UPS) described in the Office for Nuclear Regulation (ONR) “Security Assessment Principles (SyAPs) for the Civil Nuclear Industry,” (Reference 25-7), and acts as the basis of strategic intent for delivery of a robust informed design, that is measurable in accordance with the standards required in the UK.</td></tr>
<tr><th colspan="3">Security Level 2 Claims (Programme Goals)</th></tr>
<tr><th>SyL2.1 Secure-by-Design (SyBD) (UK ONR Key Security Plan Principle (KSyPP) 1)</th><th>SyL2.2 Defence in Depth (D-in-D) (UK ONR KSyPP 4)</th><th>SyL2.3 The Threat (UK ONR KSyPP 2)</th></tr>
<tr><td>The nuclear security arrangements create protection from malicious harm through a threat informed, proportionate solution, cognizant of the detail within the DBT. Security shall be an integrated component of engineering and digital architectural design that seeks to reduce vulnerabilities through minimising inherent risk, over attempting to secure or mitigate them post-design.</td><td>The nuclear security arrangements provide multiple barriers for protection against malevolent acts, including physical protection systems, engineered safety provisions, cyber protection systems, and measures for post-event management. The concept of D-in-D shall be applied to all design-related security activities to ensure they are subject to overlapping provisions, independent to the extent practicable, and that the failure of a preceding barrier shall not compromise the integrity and effectiveness of subsequent barriers.</td><td>The nuclear security arrangements are designed in cognizance and in response to counter and mitigate the modern threat environment that stems from a dynamic, intelligent adversary, who acts in a deliberate, planned fashion. Application of the DBT is used to determine these attributes and characteristics, as well as maintain presence of a credible threat in all phases of the plant design and operational lifecycles.</td></tr>
</table>

SyL2 Note	*The principal claims at Tier 2 underpin Tier 1. Defined as programme goals, these are transient requirements that are applicable in all contexts for security. These goals are key design principles that align to SyAps KSyPP (Reference 25-7). Identifiable alignment of these expectations within relevant ONR SyAPs ensures that the nuclear security solution at standard design is adoptable by prospective future UK nuclear site licence holders.*

Security Level 3 Claims (*Critical Success Factors*)		
SyL3.1 Protect against sabotage (UK ONR Fundamental Security Principle (FSyP) 6)	**SyL3.2 Protect against theft (UK ONR FSyP 6)**	**SyL3.3 Protect nuclear technology and information (UK ONR FSyP 7)**
As far as is reasonably practicable, the physical protection system shall address the design basis threat to counter and mitigate malicious acts of sabotage which could result in unacceptable radiological consequences. The physical protection system shall deliver security outcomes through the functions to: '*Deter', 'Detect', 'Delay', 'Assess', 'Respond', and 'Control of Access'*, inclusive of external and '*Insider Threat'*.	As far as is reasonably practicable, the physical protection system shall address the design basis threat to counter and mitigate the theft of nuclear/radiological material or compromise of sensitive nuclear information that could result in unacceptable radiological consequences. The physical protection system shall deliver security outcomes through the functions to: *'Deter', 'Detect', 'Delay', 'Assess', 'Respond', and 'Control of Access'*, inclusive of external and '*Insider Threat'*	As far as is reasonably practicable, the cyber protection system shall counter and mitigate malicious acts to all plant and security digital and control and instrumentation operational technology assets that could foreseeably result in: unacceptable radiological consequence, the theft of nuclear/radiological material, reduction in protective security capability, or compromise of sensitive nuclear information within information technology, through the functions of: '*Detect', 'Delay', 'Resist' and 'Recover'*.

SyL3 Note	*Tier 3 claims are defined as critical success factors and provide the claims structure the purposeful link to subsequent and underlaying arguments and evidence; and so, enabling the connective completeness of 'golden threads' from strategic intent through to operational actions, activities, and SSC important to the complete nuclear security solution.*

APPENDIX B FORWARD ACTIONS

Table B-1: Security Forward Actions

Finding	Forward Actions	Delivery Phase
Detail of the site(s) and duty holder/licensee arrangements are currently unknown. Therefore, at this stage the scope of this chapter is limited to a principles-based summary of the standard BWRX-300 design; with further supporting topic specific detail for protective security accessible within GEH Security assessment document (006N6248), as well as for cyber security within the additional material referenced within the chapter sections. As such; there is no submission titled 'Generic Security Report' (GSR). However, the submitted information and referenced documents at this point constitute the expectations of such a document, and so can be developed to suit the UK specific need of such a titled document.	GEH Security assessment document (006N6248) in completeness contains Appendices A-O, with O blank and made specifically available for international development and deployment of the BWRX-300. Appendix O will be developed to provide the UK Specific requirements, including: the UK application of categorization of security functions and classification of SSCs important to security; and detail development of site-specific and licensee/operator commitments, requirements, assumptions, and arrangements beyond the standard design.	Beyond Step 2 of GDA