GE Hitachi Nuclear Energy

NEDO-34197

Revision B

July 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 B

INFORMATION NOTICE

This document does not contain proprietary information and carries the notation “US Protective Marking: Non-Proprietary Information” and “UK Protective Marking: Not Protectively Marked.” Proprietary or UK Export Controlled Information (ECI) has been removed and is indicated by an open and closed bracket as shown here [[ ]].

IMPORTANT NOTICE REGARDING CONTENTS OF THIS REPORT
Please Read Carefully

The design, engineering, licensing, and other information contained in this document are furnished in accordance with the agreements between the UK government and GEH supporting the GDA Step 1 and 2 assessments of GEH’s BWRX-300 nuclear reactor, and nothing contained in this document shall be construed as amending or modifying the terms of such agreements. The use of this information by anyone other than the UK government, or for any purpose other than that for which it is furnished by GEH is not authorized; and with respect to any unauthorized use, GEH makes no representation or warranty, express or implied, and assumes no liability as to the completeness, accuracy, or usefulness of the information contained in this document, or that its use may not infringe privately owned rights.

UK SENSITIVE NUCLEAR INFORMATION, UK EXPORT CONTROL 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 the physical and cyber security arrangements. It sets out the arrangements that comply with the UK's legislation, regulations, and regulatory guidance.

Nuclear security includes measures to protect against malevolent actions, intended to cause unacceptable radiological releases that could affect the health and safety of the public.

This GDA covers the entire BWRX-300 design lifecycle. Many of the activities identified are deferred until a prospective operator has obtained the necessary site license and become the licensee/Dutyholder.

Claims and arguments relevant to GDA Step 2 objectives and scope are summarized in Appendix A. Appendix B, Table 25-B-1, provides a Forward Action Plan.

ACRONYMS AND ABBREVIATIONS

Acronym	Explanation
BWR	Boiling Water Reactor
CBSyS	Computer Based Security Systems
CEA	Cyber Essential Asset
CySSP	Cyber Security Plan
DBT	Design Basis Threat
DinD	Defense-in-Depth
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
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
SDLC	Software Development Lifecycle
SMR	Small Modular Reactor
SNI	Sensitive Nuclear Information
SSC	Structures, Systems and Components
SSEP	Safety, Security, and Emergency Preparedness
SyAPs	Security Assessment Principles
SyBD	Secure-by-Design
TS	Target Set
TSE	Target Set Element
UK	United Kingdom
U.S.	United States

Acronym	Explanation
VA	Vital Area
VBS	Vehicle Barrier System

TABLE OF CONTENTS

LIST OF TABLES

REVISION SUMMARY

Revision #	Section Modified	Revision Summary
A	All	Initial Issuance
B	All	Update for end of GDA Step 2 consolidation

25 SECURITY

The BWRX-300 GDA Preliminary Safety Report Chapter 25 (Security) presents at a high-level how the BWRX-300 Standard design provides a security informed design for the protection against malevolent actions, intended to cause unacceptable radiological releases that could affect the health and safety of the public. The standard design provides a robust basis for country and site-specific iteration to move to more focused detail design. The standard design provides this enabling capability through a purposeful security design philosophy and principles that are internationally recognisable.

Further detailed information regarding the protective security design can be found within 006N6248 BWRX-300 Security Assessment and is referenced throughout Chapter 25 sections to provide a linking guide to the more detailed topic information it contains. The 006N6248 BWRX-300 Security Assessment provides the detailed information that will enable a future duty holder/licensee to evolve the document into a country specific security assessment and design document that would subsequently become their nuclear site security plan.

As details of the duty holder/licensee arrangements are currently unknown, the scope of this chapter is limited to a summary and guidance of the security philosophies, principles, and methodologies 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 for UK assessment and design focus beyond Step 2 of GDA.

Appendix C provides flow diagrams of methodologies and processes.

25.1 Secure By Design

BWRX-300 is a security informed design, and from the earliest stages of product development, security has been an integral component of design and has delivered a sound basis for a Secure-by-Design (SyBD) plant at standard design that is both inherently robust and evolvable.

The goal of SyBD is to provide a significant deterrent, and a robust defensive benefit versus additional reliance on extrinsic security controls and armed personnel response; as well as minimize the operational and maintenance costs of security through better utilization of Systems, Structures and Components (SSC) (including diverse locations).

This is delivered as a cross-discipline process, ensuring integration of security into design and layout of the BWRX-300 through understanding of the ‘threat-design-outcome’ relationship, identifying and crediting security benefits inherent within the plant layout and design, passive safety systems, and managing any conflicting requirements.

The GEH Chief Engineer’s Office is the Design Authority for the BWRX-300, and SyBD is a component of primary purpose of their design oversight to:

- Prevent malicious acts (sabotage or theft) which could result in URC.
- Assure safe operations to protect people and the environment.
- Provide a design basis that can be evolved to be compliant with any national regulatory environment.

As such, GEH has established within its overall design philosophy, that robustness is a product of the underpinning intent that the BWRX-300 must be an inherently secure design as far as reasonably practical. And so, GEH seeks to reduce vulnerabilities rather than attempting to secure or mitigate them post design.

The BWRX-300 standard design demonstrates a number of engineering, layout and, technical SSC security measures that focus on what is critical for 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.
- Prevention, or ability to limit release, of radioactivity affecting public safety.

GEH approaches SyBD pragmatically, in that, identified risks are sought to be designed out; or, if that cannot be achieved, then to design-in security protective SSC to mitigate the risk. This has been enabled by progressive and repeatable formal design reviews that will continue as the design matures into country or site-specific detailed design, construction, commission, and operations.

Design is managed by a Responsible Engineer (RE) for each system design or program (e.g., Security, Isolation Condenser System, Architectural Design, Pressure Vessel, Fire Protection, HVAC). It is the RE's responsibility to coordinate the developing design with other affected areas, including security.

The Chief Engineer's Office conducts and documents formal design reviews periodically and at the end of BL-1 (Conceptual Design), BL-2 (Preliminary Design), and BL-3 (Detailed Design) to ensure the design is progressing and that the design is being properly coordinated with other design efforts. This is crucial to maintain the good practice design principles that underpin SyBD:

- Cognizance of the emerging and evolvable basis of threat.
- Defence in Depth
- Graded Approach
- A hierarchy of Security Controls
- Cross-discipline and integrated risk management
- Full-life cycle of design and operations.

Appendix C of 006N6248 BWRX-300 Security Assessment records the details of integration of SyBD to the PA, and PB building within, via the process of vulnerability assessment to evolve the structural design to support physical security and programmatic requirements. These demonstrate the outcome of security subject matter expert and engineering review and decisions to identify and mitigate vulnerabilities and to:

- Maintain security as a fundamental component of GEH design philosophy.
- Represent the cognizance of the criticality of security to safe nuclear environments.
- Ensure minimum effect on cost and maximum effect on support to security outcome performance.

Appendix K of 006N6248 BWRX-300 Security Assessment represents the GEH design and planning DBT as a set of representative scenarios against which the design and programs are evaluated to demonstrate a robust security posture. This set of scenarios is not, nor intended to be, exhaustive. As the threat environment changes, and new threat dynamics are encountered, the scenarios may be updated, or new scenarios developed.

25.2 Security Vulnerability Reviews

As a security informed design, from the earliest stages of product development of the BWRX-300 the purposeful use of vulnerability assessment, supported by cross-functional activities driven by the design oversight processes provided by the Chief Engineer's Office; has, and will continue to be used, to identify significant threats to safe operations and to provide reasonable mitigation techniques, and/or design/layout changes to the BWRX-300 to prevent significant effect to the health and safety of the public due to malicious human action.

GEH's vulnerability assessment is a design enabling process that opens the suite of security methodologies with which to:

- Determine the basis of the newly identified/introduced information and/or dynamics the design is exposed to.
- Determine how this equates into vulnerability, for what, and where.
- Determine existing standard plant, security features, and credited actions that could be applicable to mitigate it.
- Define requirements and changes to design if required.
- Identify and determine MPL stakeholder and influence and manage any conflicting requirements.

No security features are assumed to exist at the start of vulnerability assessment, to maintain an inquisitive and pragmatic approach to the new information/dynamics. As assessment continues, previously identified security features and actions may be credited through security methodologies.

Evolvability is a maintained design and operations expectation. Vulnerability assessments are a continual component of standard design evolution to ensure that emergent issues were, and will continue to be, identified, and addressed as early as possible; as well as provide the process for both gap and new analysis to introduce a basis of need for adaption and changes as the BWRX-300 design is exposed to:

- DBTs from other countries
- Site-specific threat interpretations
- Evolving understanding of threat dynamics
- DBT iteration or threat updates
- Wider MPL design, engineering, and layout updates/adaptions/changes
- Regulatory expectations
- Identification of relevant and valid International RGP
- Country or site-specific designs requirements and commitments
- New site characteristics
- The addition/update/change of technical security/safety SCC to mitigate threat and effect

This process will continue as an identified 'future work' that will be a component of commitments and requirements of future licensees and international deployment.

Of note, during the design process to standard design, the following critical 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 cladding was added 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) modules, which have 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 and/or resources for malicious activity.

25.3 General Security Design Principles

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

Further detail on the BWRX-300 Design Principles can be found within 006N6248 BWRX-300 Security Assessment: Section 7.5 and Appendices M and N (Reference 1).

25.3.1 Defense-in-Depth (DinD)

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

DinD 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.

25.3.2 Graded Approach

The application of a graded approach to the selection of security measures ensures that the resource allocations and security outcomes are proportionate to the risk, and that security SSC design, and claimed human actions are reliable, sustainable and remain valid (through evolution) for the full life of the nuclear facility and their effectiveness are supported by operational management and assurance measures.

The approach in regard to the basis of standard design is cognizant that any current evaluation of the threat is an evolvable component of consideration, and the basis of categorization determination will require exposure to sensitive nuclear information of the nation of deployment.

The standard design has used the publicly available IAEA guidance for categorization to determine basis of the nuclear material and potential consequences associated with the sabotage against nuclear material or protective SCC and the unauthorized removal of nuclear material.

25.3.3 Holistic Security Functions

GEH adopts a holistic approach to security where each aspect of security controls below 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 defense and time for onsite or offsite armed responders to interdict intruders before damage leading to severe consequences can be caused.

The security arrangements that deliver security functions include combinations of physical security, cyber security, personnel security, credited safety and security human actions, and management and leadership of procedural/behavioral controls.

These include:

- **Deter** – to discourage by instilling doubt of success and/or celerity and certainty of consequences.
- **Detect** – systems and arrangements to alert to an attempt of unauthorized entry or unauthorized act.
- **Delay** – sufficiently robust SySSC to slow progress and diminish resources to enable a response to achieve the required outcome.
- **Assess** - SySSC to enable rapid determination of suspect action and to direct an effective response.
- **Defend** - limit the ability of malicious individuals to cause damage through active and passive depletion adversary resources.
- **Control of Access** – systems and arrangements to ensure only authorized personnel can gain access to protected and restricted areas and spaces.
- **Insider Mitigation** – process and arrangements to determine if a person is acting differently to expectations, suspiciously, or out of character, to allow immediate action.

In addition, specific cyber protection system function also include:

- **Identify** – software and hardware assets, potential vulnerabilities, and determine the governance arrangements.

- **Protect** – implement measures to protect information systems to mitigate the risks identified in the cyber security risk assessment.
- **Detect** – timely indication of a potential or active cyber security incident.
- **Respond** - contain incidents, restrict connectivity, bringing systems to safe states where appropriate, communicating the incident to responders.
- **Recover** – restores systems and data, restores functionality and confidence in system performance, gathers and collates evidence.

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 will be designed with fault-tolerance in the protective security systems to ensure further effective DinD 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.

25.3.4 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.

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 defense, 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: Chapter 7 and Appendices C, F, H and K (Reference 1).

25.3.5 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.

25.3.6 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.

25.3.7 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.

25.3.8 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 Plan can be found within 006N6248 BWRX-300 Security Assessment: Chapter 8 and Appendix I (Reference 1).

25.3.9 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 defense.

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 defense 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: Chapter 9 (Reference 1). Python code used for analysis is documented in 006N6248 as part of the analysis results within Appendices C and E.

25.4 Site Characteristics, Layout, Design, and the Protected Area

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

Further details relating to the BWRX-300 site characteristics and key plant systems can be found within 006N6248 BWRX-300 Security Assessment: Chapters 4 and 5 (Reference 1).

25.4.1 Physical Environment

The BWRX-300 site consists of an access controlled and protected Exclusion Zone (EZ) where public access is restricted to only those with a valid and purposeful reason to be granted access; within which is the PA measuring approximately 200 meters by 160 meters, which is a zone further restricted to authorized 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.

Protective security is provided through a combination of a security organization, including security 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.

The PA serves to limit access to only persons who have been properly vetted and have a need for access. A visitor access program 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.

All Vital Areas (VAs) 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 DinD concepts of redundancy and physical separation of redundant systems, as well as simple passive safety systems, further support the physical protective security outcomes of the plant in that multiple vital safety and operations SSC 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.

The PA perimeter consists of a barrier with isolation zones and intrusion monitoring that surrounds all nuclear and safety 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 screening and controls 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 be qualified as a Hostile Vehicle Mitigation (HVM) barrier. A Sally Port serves as a search and screening area and ingress/egress portal for authorized vehicles with a valid need to enter.
- 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. All 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.

25.4.2 Digital Environment

GEH implements strong cyber security programs to control the system development lifecycles for all disciplines susceptible to cyber security issues, across both the Computer Based Security Systems (CBSyS) and Computer-based Systems Important to Safety (CBSIS) and other Instrumentation and Control (I&C) technology platforms. GEH's product security program is based on common industry standard frameworks such as IEC 62443 and NIST CSF 2.0, with the objective to design and achieve a layered security by design model to reduce the likelihood of unauthorized access to the plant systems of the BWRX-300.

The GEH cyber security program is designed to protect the BWRX-300 design and associated standard plant envelope from a cyber-attack or event. GEH initialized this comprehensive program at the early phases of planning to ensure SyBD and DinD are integrated to allow the licensees to take credit for the cyber security program and the security features designed into

the BWRX-300 systems. BWRX-300 incorporates fundamental 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.

25.5 Design Basis Threat (DBT)

GEH has developed a proxy Design Basis Threat (DBT) as a design and planning tool for standard design that establishes a set of credible characteristics, capabilities, and techniques for the theft or sabotage of Nuclear Material (NM) or Other Radioactive Material (ORM). This enables the BWRX-300 standard design to be matured to a robust point of basis, from which point the country specific civil nuclear DBT, and any specific site licensing threat conditions, must be applied to achieve and maintain a valid threat response and regulatory approval.

It is important to note that the use of the proxy DBT by GEH for standard design and planning purposes does not commit licensees to continued use of GEH proxy DBT in their detailed design.

The goal of the GEH DBT is to create risk reduced and robustness assurances that the country of licensure's DBT is achievable, or iteratively achievable from the standard design, and so simplify a move to the country specific DBT from the GEH proxy DBT for detailed security assessments, site-specific design, design finalization, construction, commissioning, and operational processes.

A secondary goal of the GEH proxy DBT, is that through exposure to country specific threat interpretations, it can be continuously and iteratively matured to create a more bounding case. This then subsequently enables continuous improvement at standard design, thus reducing the work required through gap analysis at the point a country specific DBT is applied.

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 threat.

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

See Annex B of this document in regard to UK future work commitments.

25.6 Categorization of NM and ORM for Theft

The primary factor in determining the physical protection measures against unauthorized removal is the nuclear material itself, and so the starting point is an analysis of the inventory and locations of NM, ORM and radioactive sources that will be present in all operation modes throughout the stations' lifecycle.

Details on the results for categorization of NM & ORM for theft review of standard plant design are contained in 006N6248 BWRX-300 Security Assessment: Section 6.2 (Reference 1).

25.6.1 Methodology for Categorization for Theft

Categorization of NM for theft for standard design has been undertaken in line with the IAEA guidance.

Identification and location of the NM and ORM inventory are critical components of determination of vital areas; as such, the process for VAI also notes categorization of the NM and ORM inventory as a component to be completed as part of that process.

25.6.2 Review of Categorization for Theft

The BWRX-300 standard design for security recognizes that evolvability needs to be considered during the lifecycle of the deployed operational plant, and so its basis is cognizant that it is likely that the activity, locations and quantities of NM, ORM and sources vary as waste is accumulated, fuel is used and operational requirements or the design changes.

Material and locations requiring protection from theft must be regularly reviewed to ensure that they remain appropriate for the site. Categorization for theft is an active process, and will also be directly triggered from events, including, but not limited to:

- A move to more detailed design beyond standard design as part of creation of country / site specific security design assessment document, and so the basis of categorization determination will require exposure to sensitive nuclear information of the nation of deployment
- Planned changes to inventory, activity, form, volume of NM, ORM or sources
- Any planned or unplanned changes to building housing NM and ORM
- Accumulation of material
- Changes to storage locations
- Amendments or changes to a nation’s categorization requirements

NOTE: Any move to country specific detailed design may also require the determining categorization values from the IAEA guidance and country regulatory expectations to be reviewed and a gap analysis to be conducted. When necessary, country specific categorization for theft values must be adopted for detailed design.

See Annex B of this document in regard to UK future work commitments.

25.6.3 NM/ORM Co-location with Other Vital Areas

In any area of the plant identified as requiring protection for theft and sabotage, the security outcome requirements should be reviewed to ensure that any potential conflicts are identified, reviewed and resolved and that both sabotage and theft-related attacks remain addressed by the security solution.

25.7 Categorization for Sabotage

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 would be capable of causing an unacceptable radiological consequence if sabotaged are designated as VAs. In addition, locations whose loss through sabotage would significantly affect the protective security or cyber security response to a threat are also included as VAs.

25.7.1 Vital Area and Target Set Identification Methodology

A complete pictorial flowchart of the Vital Area (VA) and Target Set (TS) identification process is provided in Annex C of this document to complement the narrative below.

Identification and categorization of Vital Areas, as well as identification of Target set components and Target sets, is conducted independently of both threat and any credited operator actions. Therefore, no Vital Areas, Target set components, or Target sets are, or have been, discounted as part of the development of standard design.

The BWRX-300 methodology also recognizes that other areas and SSC critical to security and operations of the plant that do not meet the regulatory definitions of a Vital Area, are also identified, classified as, and protected as Vital Areas and/or Security Sensitive Areas (SSA).

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: Chapter 6 and Appendices D and E (Reference 1).

25.7.2 Vital Area Determining Radiological Doses

GEH recognizes that countries of future deployments may utilize different determining radiological dose values at the boundary to categorize baseline, vital, and high-consequence vital areas in regard to URC. As such, country specific detailed design beyond standard design will be required to update the values utilized to meet country specific regulator expectations.

If necessary, a retrospective analysis on all existing candidate VAs (if a value delta is recognized), as well as conducting a VAI process with these figures, are undertaken to ensure no additional candidate areas are created by the change.

25.7.3 List of Vital Areas

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

25.7.4 Vital Areas and Target Set 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: Chapter 7 and Appendices H and K (Reference 1).

25.7.5 Vital Areas and Target Set Insider Mitigation

The plant security design considers the threat from an active insider that is assisting the adversarial forces, including the possibility for insider physical or cyber sabotage of critical equipment or SSC, due to coercion or affiliation.

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, behavioral observation, surveillance and monitoring in high significance areas, and information and control systems restrictions will provide a further defense against tampering.

Further detail on the BWRX-300 insider threat analysis can be found within 006N6248 BWRX-300 Security Assessment: Section 6.7.3 and Appendices A, C, and H (Reference 1).

25.8 Categorization and Classification of Security SSC

Where country specific regulatory expectations require the process of categorization and classification of security SSC, it will be a component part of country specific detailed design beyond the standard design.

See Annex B of this document in regard to UK specific forward actions and future work commitments.

25.9 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 DinD principles in a cyber security defensive architecture, which extends over the entire equipment lifecycle.

A significant threat to nuclear power plant critical systems is the insider threat which could culminate from employees, contractors, visitors and vendors which all have the potential to harm critical systems inside the nuclear plant. The harm can be both intentional and unintentional. Employees, contractors and vendors have intimate knowledge of plant equipment and networks and have the potential to cause serious damage.

Some examples of how insider threats can damage systems include but are not limited to:

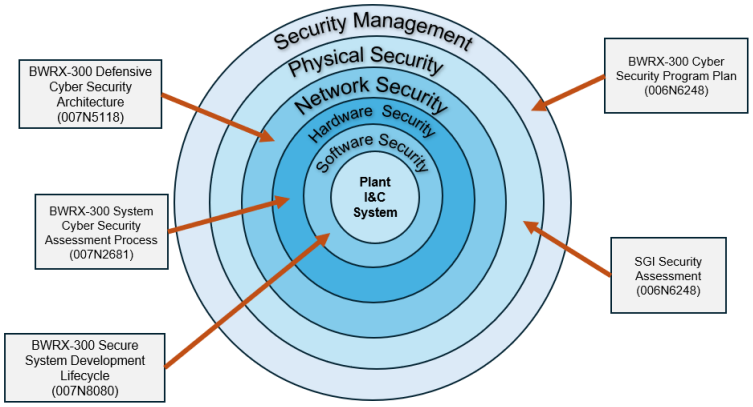
- Sabotage
- Theft
- Communication disruption
- Password disclosure
- Falsifying data
- Introducing malicious software

The cyber security program plan and other supporting cyber security governance cover the fundamental principles for cyber security controls to protect those systems and reduce the likelihood of threats such as the insider to cause damage or exploit these systems. These include but are not limited to:

- Personnel Security and Screening
- Physical Protection
- Security Awareness Training

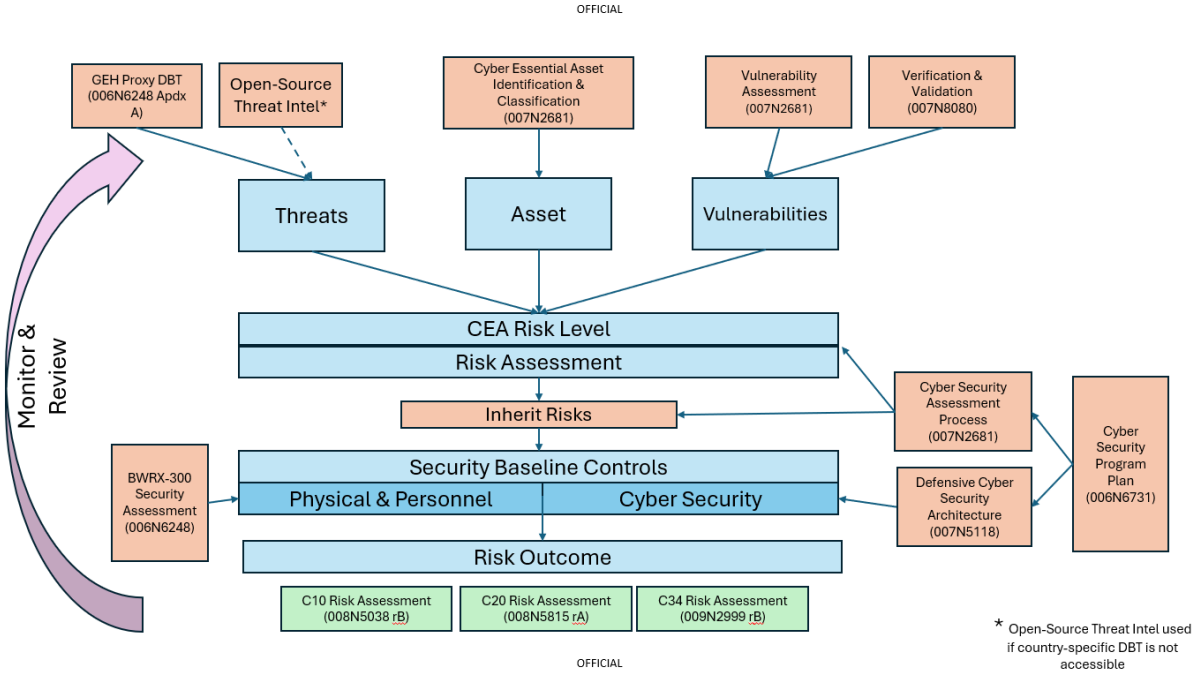
- System Hardening
- Identity and Access Management
- Security Event and Information Monitoring

BWRX-300 Plant Defense in Depth



SyBD requirements are primarily defined within the Defensive Cyber Security Architecture combined with the cyber security controls and requirements noted in the System Cyber Security Assessment Process which provides a broad overview of SyBD through DinD framework that follows NIST CSF 2.0.

The fundamental cyber security principles follow NIST cyber security framework 2.0. This framework follows 5 principles: IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER, which GEH have aligned with each core function, category and sub-category to ensure SyBD and DinD. This is captured within the Cyber Security Program Plan and the Defensive Cyber Security Architecture.



25.9.1 Cyber Security Program Plan

The 006N6731 BWRX-300 Plant Cyber Security Program Plan (CySPP) (Reference 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 CySPP 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 CySPP and other supporting cyber security requirements at the early phases of planning, to steer the design of critical systems to ensure DinD and SyBD by identifying vulnerabilities and risks at an early phase, then recommending proportionate security controls or design changes to reduce cyber risks to as low as practicable. The CySPP is a conservative set of standards that are consistent with both North American and international standards.

The BWRX-300 CySPP incorporates cyber security principles and recognized good practice throughout the development lifecycle while ensuring regulatory compliance. The objective of the CySPP 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 identifying vulnerabilities via their robust risk assessment methodology, implementing cyber security controls, and maintaining these cyber security controls throughout the system lifecycle. By design, the CySPP 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 V1.1 (Reference 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 affected due to cyber events.

The wider plan has been designed to align with required cyber security program elements from CNSC CSA 290.7.2 and NUREG-CR684 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. For UK requirements, GEH will consider adapting the CySPP and the DCSA to align to IEC 62443 or similar international standards to apply to all OT systems, in particular computer-based systems important to safety.

Furthermore, 007N8080 Cyber Security Controls for the Software Development Lifecycle (SDLC) (Reference 5) describes the process for managing cyber security risk and reducing the number of security vulnerabilities in each phase of the SDLC. For CBSIS systems, Independent verification and validation of security controls applied by an approved testing methodology to ensure prescribed controls do not degrade the safety functions or result in unnecessary transients.

GEH uses an engineering requirements management tool that includes cyber security requirements in the form of “shall” and “should” statements that inform engineering design. This tool is inherently a fundamental piece of SyBD as it allows cyber security requirements

to flow throughout all design stages for engineering deliverables. Cyber security requirements flow from regulatory requirements to create both plant wide and system specific requirements for designing digital components based on a graded approach that aligns with the agreed upon regulatory codes and standards that the BWRX-300 project is committed to.

25.9.2 Defensive Cyber Security Architecture

The 007N5118 Defensive Cyber Security Architecture (DCSA) sets the requirements for all digital systems based on their initial assessment which the process is described within the Cyber Security Assessment Process (CySAP). The DCSA is aligned to NIST CSF 2.0.

NIST CSF prescribes Defense-in-Depth by following 5 principles, IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER. The NIST framework provides a layered approach to security by the application of multiple countermeasures using people, process and technology to reduce common attack vectors and ensure that attacks missed by one control are caught by another.

The DCSA is based on the concept of DinD, by providing the requirements to build a series of defensive security layers around groups of systems with similar safety and security significance and applies defensive security measures to detect, prevent, delay, mitigate and recover from cyber-attacks. By using the DCSA requirements, this supplements the SyBD methodology but setting these requirements at the initial phases of plant design thus reducing the likelihood of introducing new vulnerabilities. The DCSA is combined with the cyber security controls and requirements outlined in the 007N2681 Cyber Security Risk Assessment.

The specification outlined in the DCSA includes the following:

- The establishment of security levels that group systems with similar cyber security requirements and safety significance based on a graded approach.
- A methodology to restrict communication flows between security levels based upon the Biba Integrity Model and ensure that communications flow unidirectionally from the highest significance security level to lowest using fail-secure, deterministic communication pathways.
- The arrangement of security levels based upon the significance, cyber security trust model, and information flows to ensure that the most significant Cyber Essential Assets (CEA)s have the greatest degree of protection.
- Based on a graded approach, common access to multiple zones and CEAs are removed to the extent possible with the remaining access monitored and controlled.
- Ensures that CEAs are logically protected by security boundaries from non-essential cyber assets.
- Where a cyber asset or a lower significance CEA’s communication with a higher significance CEA can compromise the function of the higher significance CEA, it is protected at the same level as the higher significance CEA.
- Graded requirements for the protection of systems at the security boundaries against unauthorized or malicious communications.
- The protective devices between security boundaries are graded and assigned to the most secure level they border.
- Continuous cyber security event monitoring within each security boundary and between security levels.

- Remote access communications are not permitted for high or moderate safety significance CEAs.
- Any additional requirements are necessary to meet the required level of protection.

The DCSA considers security in the design, process, controls, and tools used, through the systems engineering and software development lifecycle of the plant from planning and requirements to design, procurement, construction, and turnover to the licensee for operations and maintenance. It utilizes appropriate cyber security principles, regulatory guidance, and industry standard security models to protect the plant. Additionally, it provides a list of relevant cyber security controls required to secure identified systems based on the outcome of the risk assessment methodology, safety significance and criticality to operations.

25.9.3 Cyber Security Risk Assessment

007N2681 BWRX-300 System Cyber Security Assessment Process (Reference 3) describes the process to identify cyber critical assets which includes nuclear safety systems which may be located within vital areas or could affect nuclear safety due to a loss of availability or integrity. The outcome of this initial risk assessment will determine the Cyber Essential Asset classification which provides the cyber security assessor the safety and security significance of the proposed system, to determine appropriate baseline controls to be implemented in conjunction with the required information to perform a risk assessment to determine if the residual risks are acceptable. The baseline controls are contained within the cyber security assessment process which is aligned to the control requirements contained in the defensive cyber security architecture.

The assessment process is repeatable and performed at each phase of the system lifecycle from conceptual design through to operations.

25.9.4 Computer Based Security Systems (CBSyS)

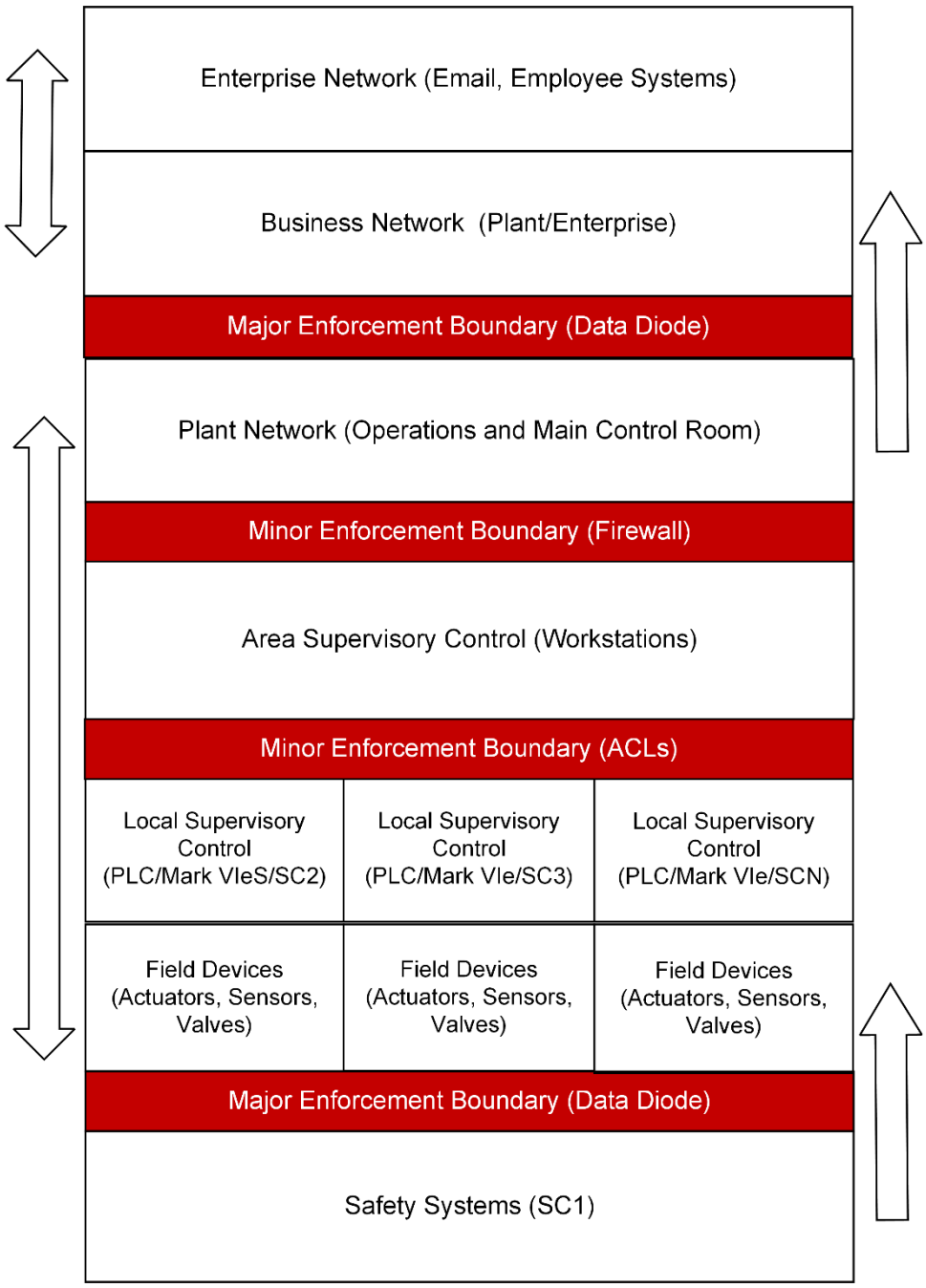
Further details on the BWRX-300 Security Computer System Cyber Security Plan can be found within 006N6248 BWRX-300 Security Assessment: Appendix G (Reference 1).

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 1).

Cyber security mitigations will be implemented during the detailed and site-specific design phases. The Cyber Security Program Plan implementation will be considered at the time of system design to ensure relevant risk assessments and controls are implemented. This will ensure the systems are SyBD and that DinD is embedded in.

25.9.5 Plant Instrumentation and Controls (I&C)

The defensive cyber security architecture to deliver SyBD and DinD of the I&C network architecture is based on recognized good practice from IEC 61513:2011 and IEC 62859. Establishing cyber security boundaries on groups of systems with similar safety and security significance provides DinD, 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 details 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 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 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 SC2, SC3, and 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 (DMZ) between IT and operational technology. This network is considered untrusted and is managed by the licensee and their IT department. The business network (DMZ) between the IT and OT networks acts as a secure intermediary that mitigates risks when connecting business IT systems to the plant's OT environments. It enforces strict access control, typically using firewalls and intrusion detection systems, to prevent direct communication between IT and OT networks while allowing essential data exchange. This segmentation reduces cyber threats, ensuring IT-based vulnerabilities don't compromise critical plant systems, such as the Primary and Diverse protection systems. Properly implemented, a DMZ supports regulatory compliance and strengthens the overall security posture of both domains.

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.

25.10 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: Chapter 3 (Reference 1).

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

25.11 Future work, Commitments, and Assumptions

GEH recognizes the continuous expectation that the effective capture of commitments and future work throughout regulatory design assessment processes as well as its own internally identified commitments and future work required of country specific deployments, is a vital enabler of future design and regulatory activities and progressing the design and the security reports to a Nuclear Site Security Plan (NSSP).

See Annex B of this document in regard to UK specific forward actions and future work commitments.

25.12 References

1. BWRX-300 Security Assessment, 006N6248 Rev 2.
2. BWRX-300 Plant Cyber Security Program Plan, 006N6731 Rev 2.
3. BWRX-300 System Cyber Security Assessment Process, 007N2681 Rev C.
4. BWRX-300 Defensive Cyber Security Architecture, 007N5118 Rev C.
5. Cyber Security Controls for the Software Development Lifecycle, 007N8080 Rev A.
6. BWRX-300 UK GDA Safety Case Development Strategy, NEDC-34140P.
7. Security Assessment Principles for the Civil Nuclear industry, Office for Nuclear Regulation, 2022 Edition, Version 1.
8. NIST Cyber Security Framework V1.1.
9. IEC 61513:2011, Nuclear Power Plants – Instrumentation and Control Important to Safety – General Requirements for Systems, International Electrotechnical Commission.
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 the Safety Case Development Strategy (Reference 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 25-A-1.

Table 25-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 ONR SyAPs (Reference 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 KSyPP 1)</th><th>SyL2.2 Defense in Depth (DinD) (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 defense-in-depth 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 Design Basis Threat (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 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 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

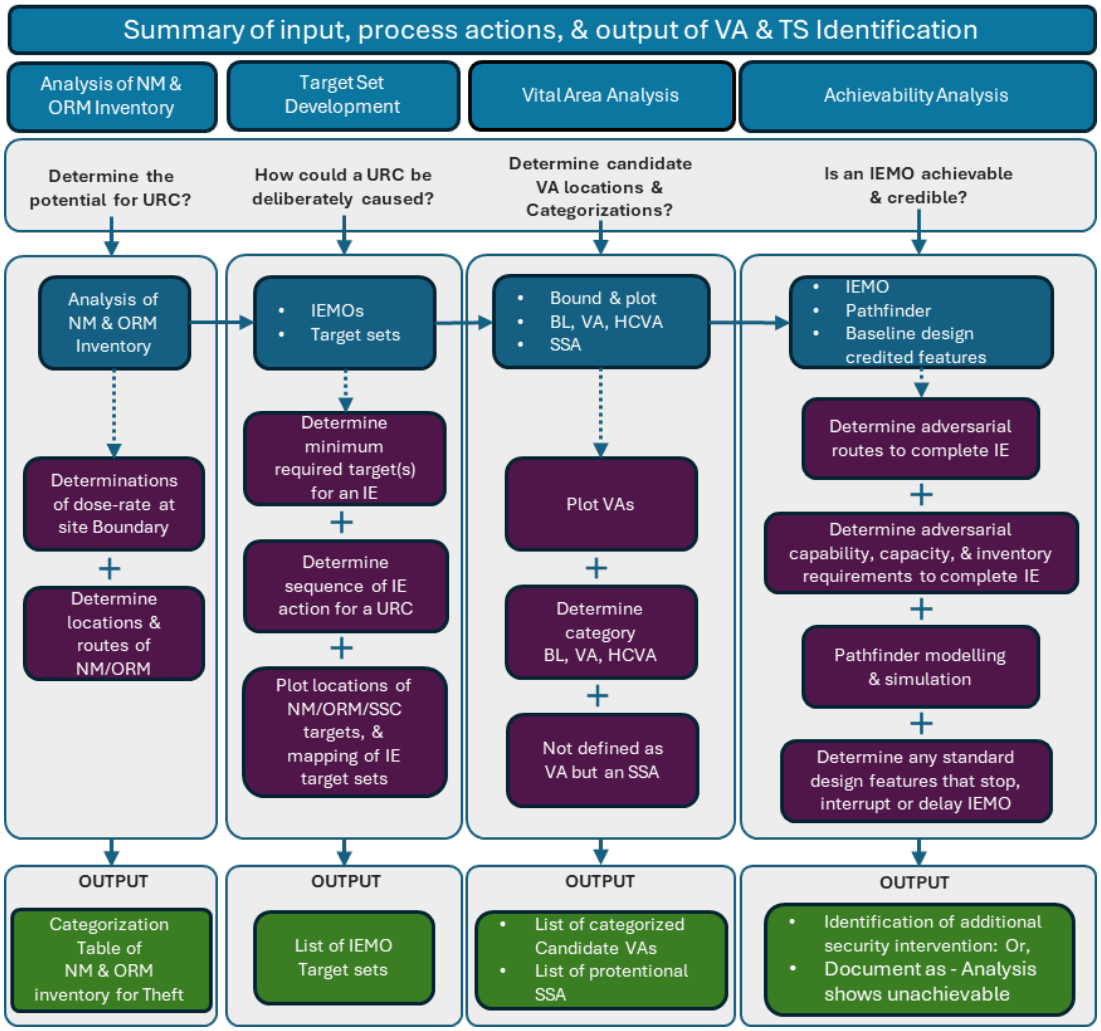
Table 25-B-1: Security Forward Actions

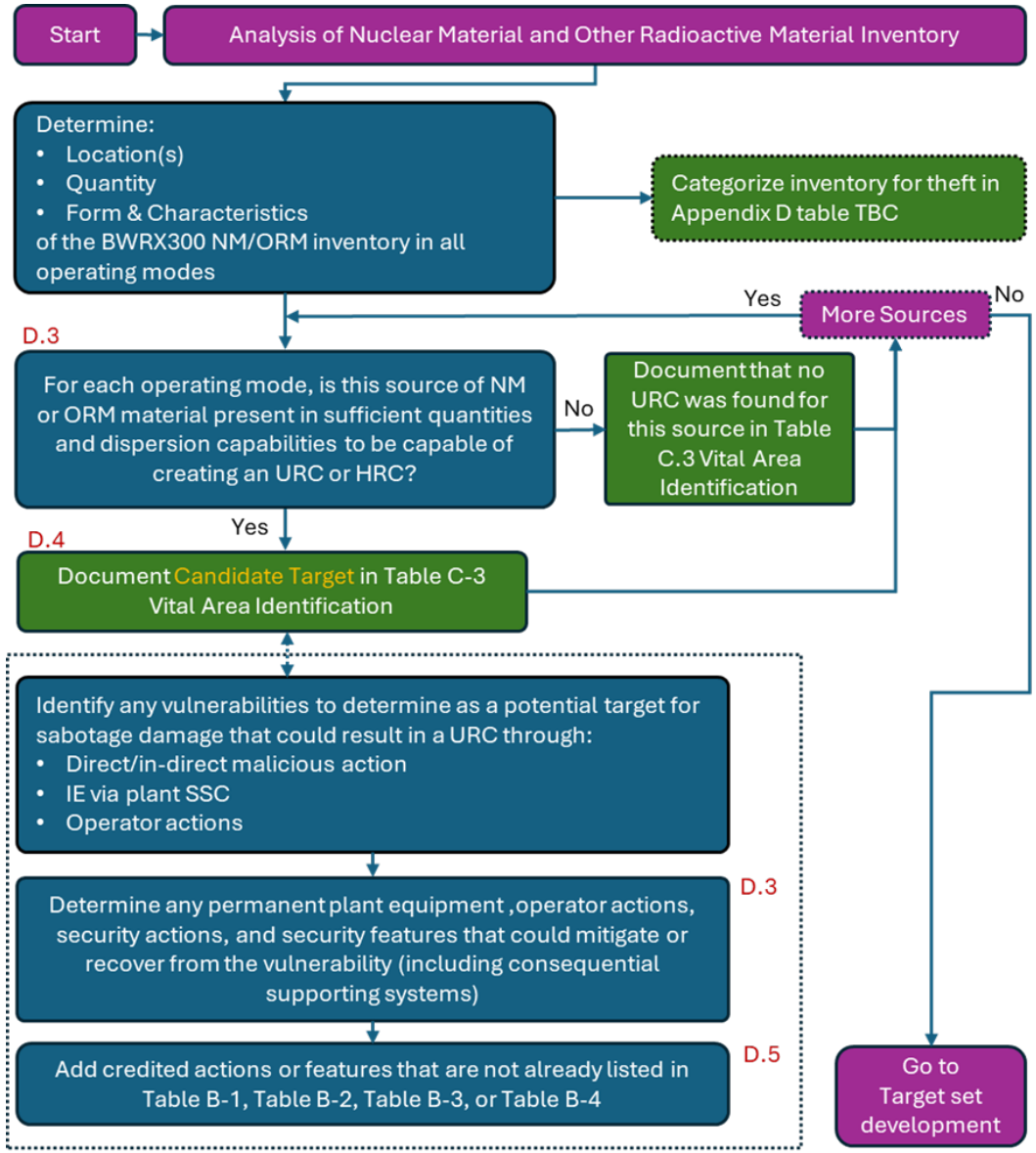
Forward Actions	Delivery Phase
Licensee / DevCo leading UK specific detailed design must use the UK-DBT beyond Step 2 of GDA. This includes any UK specific requirements applicable for a more detailed design or assessment for either further GDA steps or site specific design. Appendix A of the Security Assessment will be replaced at this point by UK-DBT and a vulnerability gap analysis of BL-0 standard design utilising the UK threat interpretation. All further future security work for UK specific detailed design requiring use of a threat interpretation will use this updated Appendix.	Before Site License Application, and/or BL3 Design Phase
Beyond Step 2 of GDA, and as basis values differ between IAEA and ONR expectations, the Licensee / DevCo leading UK specific detailed design must replace basis of categorization for theft values to the information contained within SyAPs OS-SNI Annex A, tables 1-3, review (and update if necessary) current determinations, and progress using the UK specific data for all future assessments of the NM and ORM inventory.	Before Site License Application, and/or BL3 Design Phase
Licensee / DevCo leading UK specific detailed design beyond standard design will be required to update the determining radiological dose values at the boundary to categorise baseline, vital, and high-consequence vital areas in regard to URC to meet the UK regulator expectations (SyAPs OS-SNI Annex B, table 1) and conduct a retrospective analysis on all existing candidate VAs; as well as conduct a VAI process with these figures to ensure no additional candidate areas are created by the change. In addition, other areas critical to, and sensitive to, security and operations of the plant that do not meet the regulatory definitions of a Vital Area, are also identified, classified as, and protected as Vital Areas and/or Security Sensitive Areas (SSA).	Before Site License Application, and/or BL3 Design Phase
Commitment upon Licensee / DevCo to iteratively complete categorization of security functions and classification of SSC important to security alongside development of detailed design for UK specific deployment.	Before Site License Application, and/or BL3 Design Phase

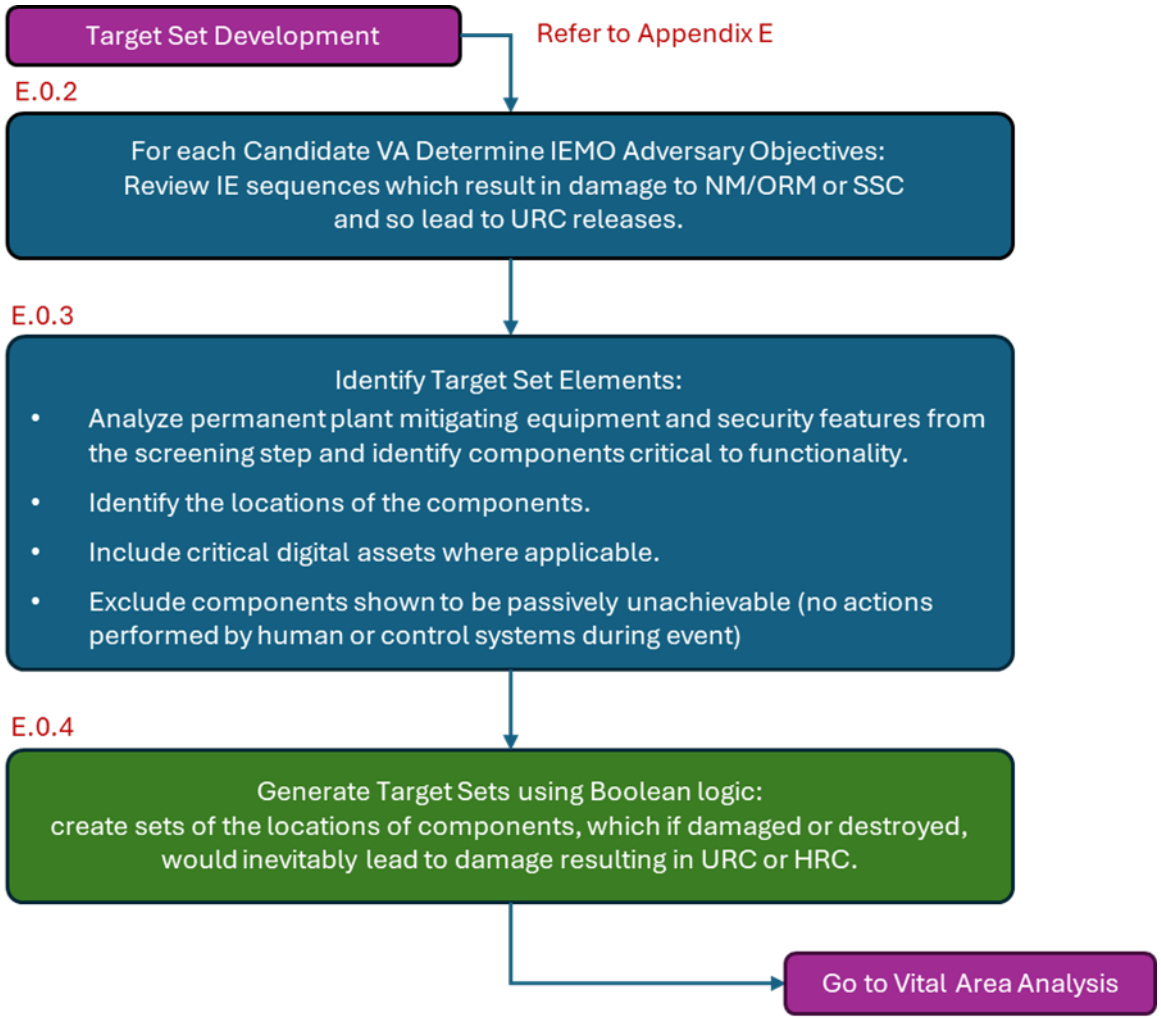
Forward Actions	Delivery Phase
Cyber Security Future Commitments - Future revision of the CSAP to align to a relevant International standard for OT cyber security such as IEC 62443, NIST CSF 2.0 or NIST SP 800-82. - A review of the existing cyber security documentation governance, in particular the Defensive Cyber Security Architecture, will be undertaken with the aim to form the DCSA into a policy or standard document that defines what controls must be in place on critical digital assets. DCSA currently doesn't define the requirements for RBAC and IAM. - For site specific design phase, it will be considered to revise the plant design to meet UK regulatory requirements which recommends implementing a defined and robust DMZ between the enterprise IT network and Level 3 of the plant network.	Before Site License Application, and/or BL3 Design Phase

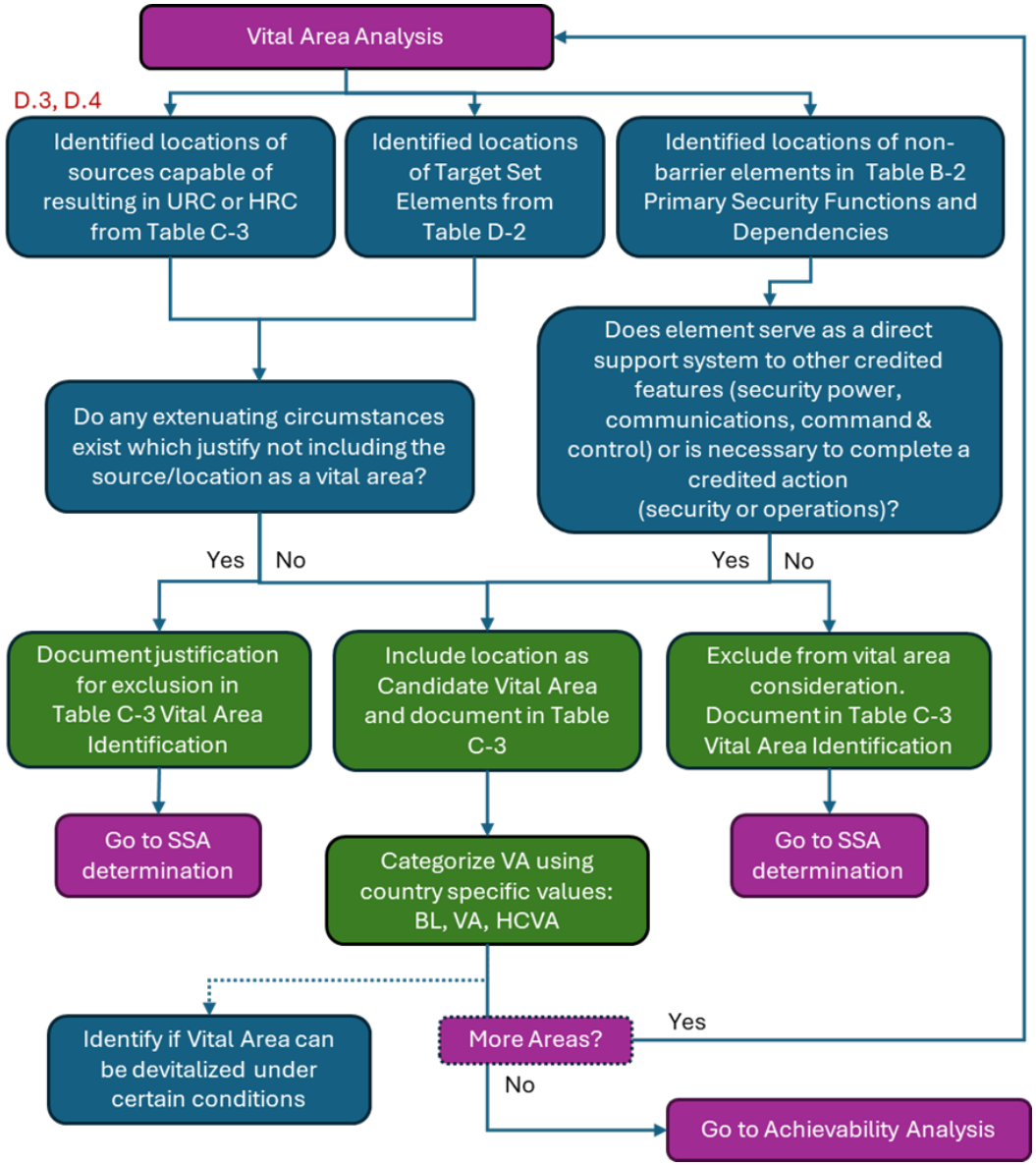
APPENDIX C FLOW CHARTS

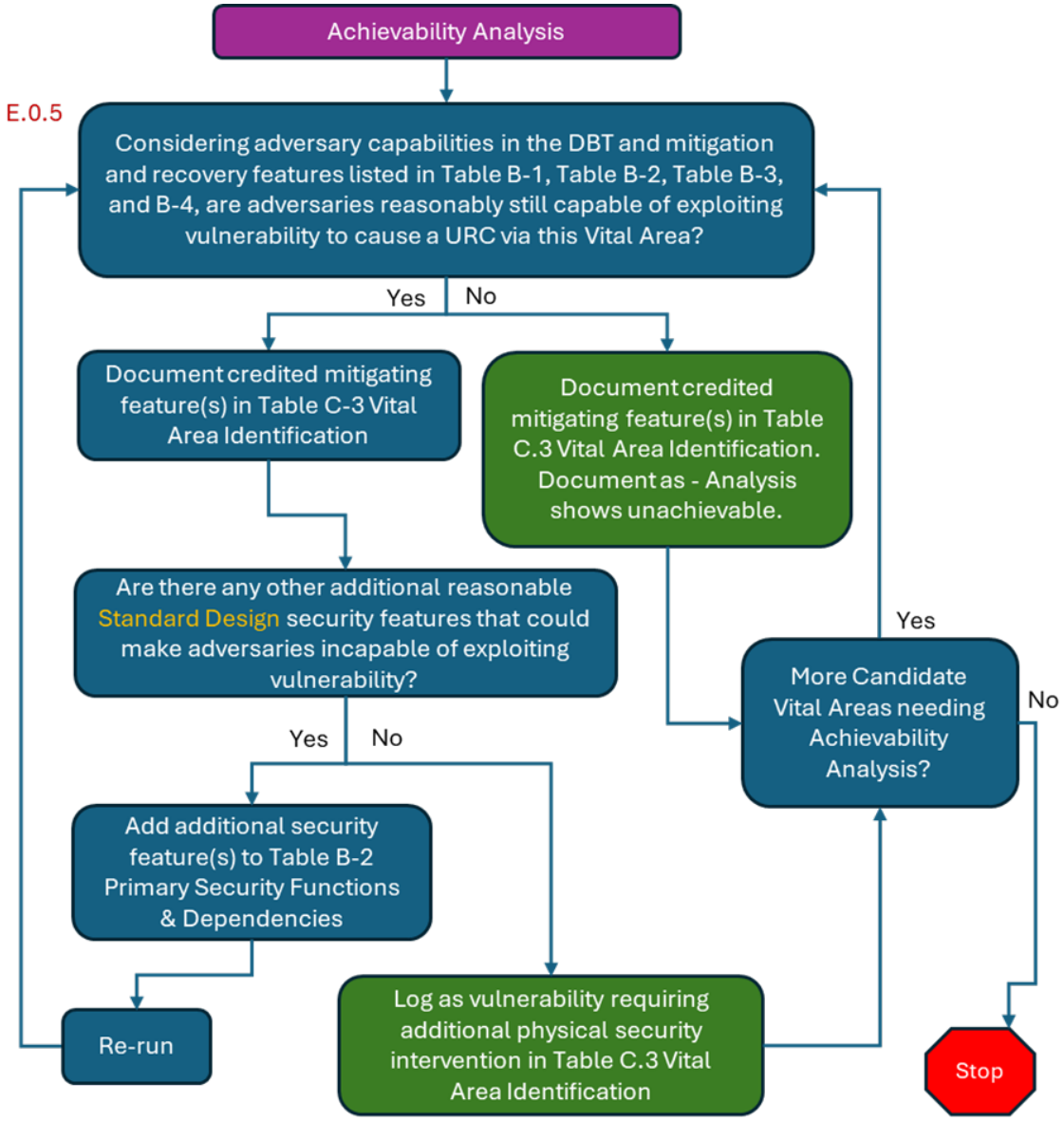
Vital Area & Target Set Identification:

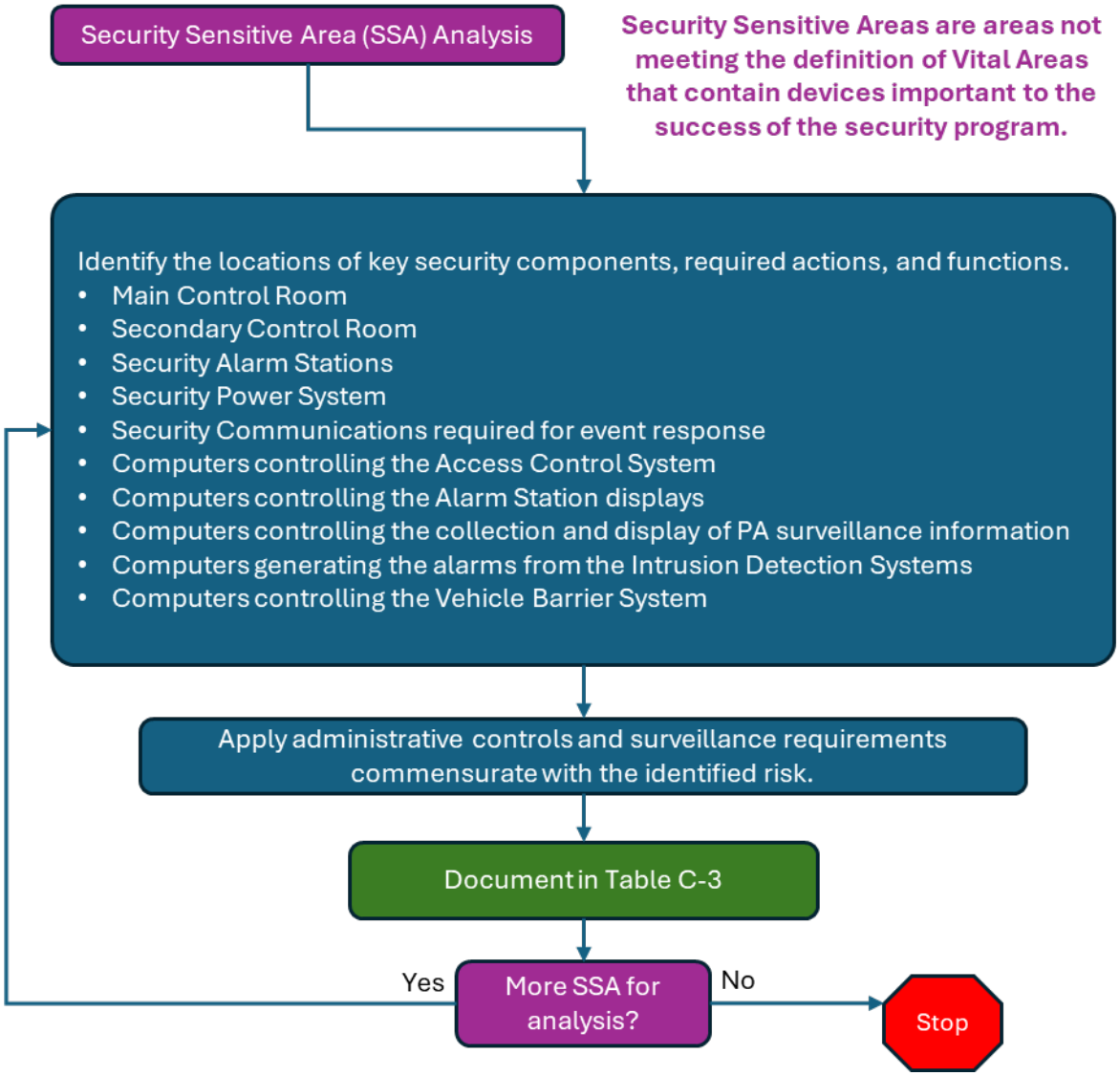



Start
Analysis of Nuclear Material and Other Radioactive Material Inventory
Determine:
• Location(s)
• Quantity
• Form & Characteristics
of the BWRX300 NM/ORM inventory in all operating modes
Categorize inventory for theft in Appendix D table TBC
Yes
More Sources
No
D.3
For each operating mode, is this source of NM or ORM material present in sufficient quantities and dispersion capabilities to be capable of creating an URC or HRC?
No
Document that no URC was found for this source in Table C.3 Vital Area Identification
Yes
D.4
Document Candidate Target in Table C-3 Vital Area Identification
Identify any vulnerabilities to determine as a potential target for sabotage damage that could result in a URC through:
• Direct/in-direct malicious action
• IE via plant SSC
• Operator actions
Determine any permanent plant equipment ,operator actions, security actions, and security features that could mitigate or recover from the vulnerability (including consequential supporting systems)
D.3
Add credited actions or features that are not already listed in Table B-1, Table B-2, Table B-3, or Table B-4
D.5
Go to Target set development


Target Set Development
Refer to Appendix E
E.0.2
For each Candidate VA Determine IEMO Adversary Objectives:
Review IE sequences which result in damage to NM/ORM or SSC
and so lead to URC releases.
E.0.3
Identify Target Set Elements:
Analyze permanent plant mitigating equipment and security features from the screening step and identify components critical to functionality.
Identify the locations of the components.
Include critical digital assets where applicable.
Exclude components shown to be passively unachievable (no actions performed by human or control systems during event)
E.0.4
Generate Target Sets using Boolean logic:
create sets of the locations of components, which if damaged or destroyed, would inevitably lead to damage resulting in URC or HRC.
Go to Vital Area Analysis


Vital Area Analysis
D.3, D.4
Identified locations of sources capable of resulting in URC or HRC from Table C-3
Identified locations of Target Set Elements from Table D-2
Identified locations of non-barrier elements in Table B-2 Primary Security Functions and Dependencies
Do any extenuating circumstances exist which justify not including the source/location as a vital area?
Does element serve as a direct support system to other credited features (security power, communications, command & control) or is necessary to complete a credited action (security or operations)?
Yes
No
Yes
No
Document justification for exclusion in Table C-3 Vital Area Identification
Include location as Candidate Vital Area and document in Table C-3
Exclude from vital area consideration. Document in Table C-3 Vital Area Identification
Go to SSA determination
Categorize VA using country specific values: BL, VA, HCVA
Go to SSA determination
Identify if Vital Area can be devitalized under certain conditions
More Areas?
Yes
No
Go to Achievability Analysis


Achievability Analysis
E.0.5
Considering adversary capabilities in the DBT and mitigation and recovery features listed in Table B-1, Table B-2, Table B-3, and B-4, are adversaries reasonably still capable of exploiting vulnerability to cause a URC via this Vital Area?
Yes
No
Document credited mitigating feature(s) in Table C-3 Vital Area Identification
Document credited mitigating feature(s) in Table C.3 Vital Area Identification. Document as - Analysis shows unachievable.
Are there any other additional reasonable Standard Design security features that could make adversaries incapable of exploiting vulnerability?
Yes
No
Add additional security feature(s) to Table B-2 Primary Security Functions & Dependencies
Re-run
Log as vulnerability requiring additional physical security intervention in Table C.3 Vital Area Identification
More Candidate Vital Areas needing Achievability Analysis?
Yes
No
Stop


Security Sensitive Area (SSA) Analysis
Security Sensitive Areas are areas not meeting the definition of Vital Areas that contain devices important to the success of the security program.
Identify the locations of key security components, required actions, and functions.
• Main Control Room
• Secondary Control Room
• Security Alarm Stations
• Security Power System
• Security Communications required for event response
• Computers controlling the Access Control System
• Computers controlling the Alarm Station displays
• Computers controlling the collection and display of PA surveillance information
• Computers generating the alarms from the Intrusion Detection Systems
• Computers controlling the Vehicle Barrier System
Apply administrative controls and surveillance requirements commensurate with the identified risk.
Document in Table C-3
Yes
More SSA for analysis?
No
Stop