| Revision | Approved by | Number of Pages |
|---|---|---|
| 000 | | 104 |
| **Approval Date** | 07/02-20 | |

CGN EDF
General Nuclear System

# General Nuclear System Ltd.

UK HPR1000 GDA Project

| **Document Reference:** | **HPR/GDA/GSR/0002** |
|---|---|

**Title:**

# Generic Security Report – Security Case (DR1)

# Version 1 (Public)

This document has been prepared on behalf of General Nuclear System Limited with the support of China General Nuclear Power Corporation (CGN) and Électricité de France S.A. (EDF).

Although due care has been taken in compiling the content of this document, neither General Nuclear System Limited, CGN, EDF nor any of their respective affiliates accept any liability in respect to any errors, omissions or inaccuracies contained or referred to in it.

Text within this document that is enclosed within brackets '{…}' is Sensitive Information and is not to be disclosed to any third party without written consent of General Nuclear System Limited.

# DISTRIBUTION LIST

| Recipients | Cross Box |
|---|---|
| General Nuclear System Executive | ☒ |
| General Nuclear System all staff | ☐ |
| General Nuclear System and BRB all staff | ☐ |
| CGN | ☐ |
| EDF | ☐ |
| Regulators | ☒ |
| Public | ☒ |

# DISTRIBUTION LIST

| Recipients | Cross Box |
|---|---|
| General Nuclear System Executive | ☒ |
| General Nuclear System all staff | ☐ |
| General Nuclear System and BRB all staff | ☐ |
| CGN | ☐ |
| EDF | ☐ |
| Regulators | ☒ |
| Public | ☒ |

# MODIFICATION RECORD

| Revision | Section | Page | Modification |
|---|---|---|---|
| 000 | ALL | ALL | First Issue |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

# TABLE OF CONTENTS

# 1. List of Abbreviations and Acronyms

| | |
|---|---|
| BRB | Bradwell B |
| CAE | Claims, Arguments and Evidence |
| CBSIS | Computer Based Systems Important to Safety |
| CBSy | Computer Based Security Systems |
| CGN | China General Nuclear Power Corporation |
| CONOP | Concept of Operation |
| CPS | Cyber Protection System |
| CSRA | Cyber Security Risk Assessment |
| DAC | Design Acceptance Confirmation |
| DBT | Design Basis Threat |
| EDF | Électricité de France |
| FCG3 | Fanchenggang 3 |
| FSF | Fundamental Safety Function |
| FSyP | Fundamental Security Principle |
| GDA | Generic Design Assessment |
| GNI | General Nuclear International |
| GSR | Generic Security Report |
| HMG | Her Majesty's Government |
| HMI | Human Machine Interface |
| HPR | Hualong Pressurised Reactor |
| HSA | Hostile State Actor |
| IAEA | International Atomic Energy Agency |
| I&C | Instrumentation and Control |
| IEMO | Initiating Event of Malicious Origin |
| IT | Information Technology |
| KSyPP | Key Security Plan Principle |

| | |
|---|---|
| NIMCA | Nuclear Industries Malicious Capability Planning Assumptions |
| NM | Nuclear Material |
| NPP | Nuclear Power Plant |
| NSSP | Nuclear Site Security Plan |
| NU | Normal User |
| ONR | Office for Nuclear Regulation |
| ORM | Other Radioactive Material |
| OT | Operational Technology |
| PCER | Pre-Construction Environmental Report |
| PCSR | Pre-Construction Safety Report |
| PPS | Physical Protection System |
| PIE | Postulated Initiating Event |
| PSAS | Plant Standard Automation System |
| PSM | Protective Security Measure |
| PU | Privileged User |
| PWR | Person Within Range |
| RGP | Relevant Good Practice |
| RP | Requesting Party |
| SA | Security Architecture |
| SEC | Sabotage Event Combination |
| SF | Spent Fuel |
| SI | Security Infrastructure |
| SISC | Security In Supply Chain |
| SL | Site Licensee |
| SNI | Sensitive Nuclear Information |
| SQEP | Suitably Qualified and Experienced Person |
| SSC | Structure, System & Component |
| SSER | Safety, Security and Environmental Report |

| | |
|---|---|
| SyAPs | Security Assessment Principles |
| SyDP | Security Delivery Principle |
| UK HPR | United Kingdom Hualong Pressurised Reactor |
| URC | Unacceptable Radiological Consequence |
| USB | Universal Serial Bus |
| VA | Vital Area |
| VAI | Vital Area Identification |
| VAIM | Vital Area Identification Methodology |

## 2. Executive Summary

The UK HPR1000 is undergoing a Generic Design Assessment (GDA) in the UK with the Office for Nuclear Regulation (ONR); this is a four-step process to obtain design approval for the use of a new nuclear reactor design within the UK. General Nuclear System Limited acts on behalf of the Requesting Party (RP) to lead the GDA, and will be referred to as the RP throughout this document.

The purpose of the GDA is to gain a Design Acceptance Confirmation from ONR and a Statement of Design Acceptance from the Environment Agency for the generic design of the reactor. These will be achieved if the RP submits a satisfactory Safety, Security and Environmental Report (SSER) to the Regulators.

The Generic Security Report – Security Case (GSR-SC) forms part of the SSER and will identify the Nuclear Material and Other Radioactive Material within the Nuclear Power Plant that could be stolen or sabotaged. It will also identify physical and Operational Technology assets that maintain the material in a safe condition and need protection against a physical and cyber threat capability that could cause the sabotage or theft. The areas around these assets are identified as Vital Areas and will be categorised in levels of importance. Proportionate layers of security will be developed to protect the Vital Areas and to provide defence in depth. This report, the GSR–SC (Public) (GSR-SC(P)), is a redacted version of the GSR-SC and it has been made publicly available by removing some sections from the original in the interests of national security.

This submission (Version 1) of the GSR-SC(P) is made at the end of Step 3 of the GDA process has been written against Design Reference 1 for the UK HPR1000 and so the security assessment is not complete. The report will be developed throughout Step 4 of GDA, when the Protective Security Measures to protect Vital Areas will be developed, together with the Concept of Operation for the delivery of the security measures.

Once complete, the GSR will provide evidence that the security measures for the UK HPR1000 will deliver outcomes to satisfy the regulatory expectations within ONR's Security Assessment Principles (SyAPs) (Reference [1]). The GSR-SC(P) will support these activities by following the 'secure by design' principle to design-out security vulnerabilities where appropriate, and list the assumptions, commitments and requirements that have been identified.

It will also form the basis for the development of the site-specific Nuclear Site Security Plan (NSSP) that will be prepared by the future Licensee.

# 3. Introduction

The UK HPR1000 is an evolutionary design of advanced Nuclear Power Plant (NPP) which incorporates an active and passive safety design philosophy. It combines proven technology from existing Pressurised Water Reactors (PWRs) with advanced design features, active and passive safety systems, comprehensive severe accident prevention and mitigation measures, enhanced protection against external events and improved emergency response capability.

The reference design for the UK HPR1000 is the Hualong Pressurised Reactor (HPR) currently under construction at Fangchenggang NPP Unit 3 (FCG3) in southern China. This is a three-loop PWR-based technology systematically modified and developed based on successful operation of the Chinese PWR fleet.

The Generic Security Report – Security Case (GSR-SC) is part of the Safety, Security and Environmental Report (SSER), which represents the security aspects of the UK version of the Hua-long Pressurised Reactor (UK HPR1000).

The SSER also comprises the Pre-Construction Safety Report (PCSR) (Reference [2]) and Pre-Construction Environmental Report (PCER) (Reference [3]), which together present the safety and environmental assessment of the proposed design. The SSER aims to demonstrate that the design of the UK HPR1000 is suitable for its intended construction, commissioning, operation and ultimate decommissioning on a generic site in the UK.

The Requesting Party (RP) for the UK HPR1000 Generic Design Assessment (GDA) process jointly comprises China General Nuclear Power Corporation (CGN), Électricité de France S.A. (EDF S.A.) and General Nuclear International (GNI). General Nuclear System Limited is appointed by the above shareholders to act on behalf of the RP. The General Nuclear System Limited Shareholder Agreement sets out the full specification of the governance arrangements and decision-making processes for GDA. For the purposes of clarity, General Nuclear System Limited will be referred to as the RP throughout this document.

The RP is required to develop a comprehensive, generic security case, comprising the GSR and including relevant supporting reference documents as guided in ONR's New Nuclear Power Plants: Generic Design Assessment Guidance to Requesting Parties (Reference [4]). In summary, the GSR-SC will describe the security features of the proposed design and it will document the categorisation of Nuclear Material/Other Radioactive Material (NM/ORM) from both theft and sabotage to determine the protective security outcomes and applicable security postures to be applied. Regulatory security expectations are described within ONR's Security Assessment Principles (SyAPs) (Reference [1]), in the form of Fundamental Security Principles (FSyPs), Security Delivery Principles (SyDPs) and Key Security Plan Principles (KSyPPs). The GSR will provide evidence that the security measures for the UK HPR1000 will deliver

outcomes that will satisfy these regulatory expectations. This document, together with supporting reference documents, fulfils this requirement but it is a redacted version of the full report. Certain items of information have been redacted in the interests of national security to enable the GSR-SC(P) to be made publicly available. Information presented in italicised font indicates where sensitive information has been redacted. The rationale behind this exercise has been to:

- keep the public informed of the security considerations that have been undertaken;
- show the methodology that has been devised to identify those areas that need security protection; and
- give the public confidence that an appropriate and robust security case to protect the NPP will be proposed.

It is important to note that the GSR, together with the supporting reference documents, has been written using design information available under Design Reference 1 and at the end of Step 3 of the GDA programme. It will be further developed throughout Step 4 of the GDA.

To complete its assessment, the GSR will identify the locations of NM/ORM that needs to be protected from theft and sabotage, the physical and OT assets that keep the material in a safe condition, the locations of these assets as Vital Areas, and finally, layers of proportionate security measures to achieve the security outcomes that are required. The levels of maturity of information used in the assessment will vary and so the GSR will also identify any assumptions that it has made, commitments to progress the assessment and requirements for further information.

This document will form the basis of site-specific security planning that will be passed onto any future Site Licensee (SL).

# 4. Purpose

The purpose of the GSR is to support the award of a Design Acceptance Confirmation (DAC) from the Regulator at the end of the GDA programme. To do this, it will describe the security features of the UK HPR1000 reactor technology as the security element of the SSER, and directly to support the delivery the UK HPR1000's Fundamental Objective for GDA:

The ***Fundamental Objective*** of the UK HPR1000 is that: *The Generic UK HPR1000 could be constructed, operated, and decommissioned in the UK on a site bounded by the generic site envelope in a way that is safe, secure and that protects people and the environment.*

In doing so, the GSR will document the categorisation of Nuclear Material (NM) and Other Radioactive Material (ORM) from both theft and sabotage in order to determine the protective security outcomes and applicable security postures to be applied. It will also identify and characterise equipment or software used on the premises in connection with activities involving NM/ORM in order to determine the cyber security outcomes and applicable cyber security postures to be applied.

The security measures identified will be graded, provide defence-in-depth and meet regulatory expectations in respect of SyAPs. In this way, the GSR will support the development of a future site-specific security plan (that will be delivered by the SL) as required in ONR's New Nuclear Power Plants: Generic Design Assessment Technical Guidance (Reference [5]).

# 5. Objectives

The objectives of the GSR are to support the delivery of a security-informed design of the UK HPR1000 that protects the nuclear inventory from sabotage and theft, and may be described as follows:

(1) Identification of the nuclear inventory within the GDA scope and its location.

(2) Categorisation of the nuclear inventory for sabotage and theft.

(3) Identification of the assets requiring protection to prevent the sabotage and theft of the nuclear inventory, together with their locations and potential sabotage combinations.

(4) Identification and location of the OT that could facilitate the sabotage of the assets via the introduction of a cyber threat.

(5) Development and application of a GDA Design Basis Threat (DBT) for Physical and Cyber Security from NIMCA, Reference [10].

(6) Identification and consideration of potential plant design solutions to eliminate or reduce the potential for sabotage and/or theft of the nuclear inventory.

(7) Development of a list of areas for protection against theft and sabotage, suitably categorised and classified for security purposes.

(8) Definition of protection against theft and sabotage via a combination of proportional physical, cyber and procedural measures.

(9) Establishment of a concept of security operations to provide defence-in-depth, proportional security and an effective security culture.

# 6. Scope

The overall scope for the UK HPR1000 GDA project is presented in Scope for UK HPR1000 GDA Project, Reference [6].

Within these boundaries, the scope for the GSR is to describe the security features of the UK HPR1000 reactor technology in sufficient detail to enable the Regulator to complete a meaningful assessment. A meaningful assessment, as defined in Reference [5], will be one where ONR has:

a) Received sufficient information in the GSR to allow assessment in all relevant technical assessment topics that cover the full breadth and depth necessary for ONR to carry out its intended assessments;

b) Completed an appropriately thorough and detailed assessment of that information on a sampling basis, and judged it against applicable standards and guidance.

To support a meaningful assessment, the GSR presents a comprehensive, generic security case, comprised of this head document with relevant supporting reference documents. Guidance on the scope of the GSR has been drawn from ONR's Guidance on the Security Assessment of Generic New Nuclear Reactor Designs (Nuclear Security Technical Assessment Guide 11.1) (Reference [7]) and further details on the scope are listed below:

a) The security arrangements detailed in the GSR will meet regulatory expectations in respect of the FSyPs.

b) Sufficient information will be provided to enable the Regulator to make an informed judgement on the adequacy of the security aspects of the generic design, to support the construction and subsequent operation of the technology in the UK.

c) Where claims are made on the adequacy of security arrangements which take into account those measures to be determined by the SL, e.g. perimeter fences, gatehouse, hostile vehicle mitigation, personnel security etc, there will be clear statements explaining how the potential licensee's arrangements are expected to combine with those of the GSR to mitigate against these threats.

d) The GSR will clearly describe where all of the relevant KSyPPs and SyDPs have been addressed and provide evidence to this effect.

e) The GSR will make claims on the safety case and environmental case as appropriate, and it will provide evidence to show integration across the SSER.

f) The scope of the plant under assessment within the GSR will be clearly stated.

g) The GSR will identify all targets within the NPP and categorise them

appropriately for theft and sabotage.

h) Security outcomes will be derived from the target categorisation above, and a DBT will be defined and applied to ensure that the proposed security architecture and security infrastructure are proportionate and effective in meeting the appropriate SyAPs outcomes.

i) Defence-in-depth is recognised as a KSyPP and the GSR will illustrate the concept of several layers and methods of protection to deliver the required security outcomes.

j) The security assessment will be conducted on the extant Design Reference at the time of the assessment, and it will be based on the maturity of design at that point.

The structure of the GSR that will deliver all of the elements that have been described as being within scope of the security case is explained in detail at Section 8 of this report.

# 7. Claims, Arguments and Evidence

## 7.1 Background

Within the SSER documents, a 'Claims, Argument, Evidence' (CAE) approach has been adopted in order to develop a 'route map' for the safety case documentation (Reference [2]).

The benefits of adopting this approach to claims within the security assessment are considered to be threefold; firstly, adopting a CAE approach has benefits in terms of providing a top-down assessment of what is to be achieved to meet the fundamental objective through a cascade of claims to arguments and, finally, to evidence. Therefore, such a top-down approach can be used to establish the completeness of the work to be undertaken to meet the fundamental objective.

The second benefit of such an approach is that it gives an underlying structure to the resultant documentation throughout the proposed three tier approach. Hence by developing a structured, clear and logical CAE approach for security claims within the GSR, it will be clear how the relevant arguments and evidence are addressed and where this is achieved in the document structure. This will also have benefits in the communication of such claims to the rest of the project and other stakeholders.

Finally, adopting a CAE for the GSR enables the security CAE to be integrated with the safety and environmental CAE. This demonstrates the integrated nature of the project and widens visibility of the GSR within the overall GDA project. Hence, the approach adopted in developing security-based CAEs is to integrate with the SSER CAE to yield the benefits of such integration.

## 7.2 Approach

The approach adopted is to firstly review the existing CAE route map to identify relevant existing claims. These have been reviewed for completeness and augmented as necessary.

Following the establishment of high-level claims, lower level sub-claims have been developed which reflect the more specific claims to be met by the GSR assessment. These claims and sub-claims comprise a structured breakdown of the higher-level claims such that achievement of the lower level claims will indicate achievement of the higher level claim.

The approach and language used in the developed sub-claims, arguments and evidence is similar in style, depth and terminology to those presented in the SSER for consistency with the rest of the GDA project.

### 7.3 Development of Claims, Argument, Evidence for the Generic Security Report

The UK HPR1000 has the following Fundamental Objective:

**Fundamental Objective:** *The Generic UK HPR1000 could be constructed, operated, and decommissioned in the UK on a site bounded by the generic site envelope in a way that is safe, secure and that protects people and the environment.*

Beneath this fundamental objective, the SSER has developed a number of Level 1 Claims. These have been reviewed and a number highlighted as being relevant to the security assessment. These are:

- Level 1 Claim 2, which covers organisational arrangements for the SSER documentation and hence is also applicable to the GSR
- Level 1 Claim 4, which addresses security as a specific aspect of the SSER.

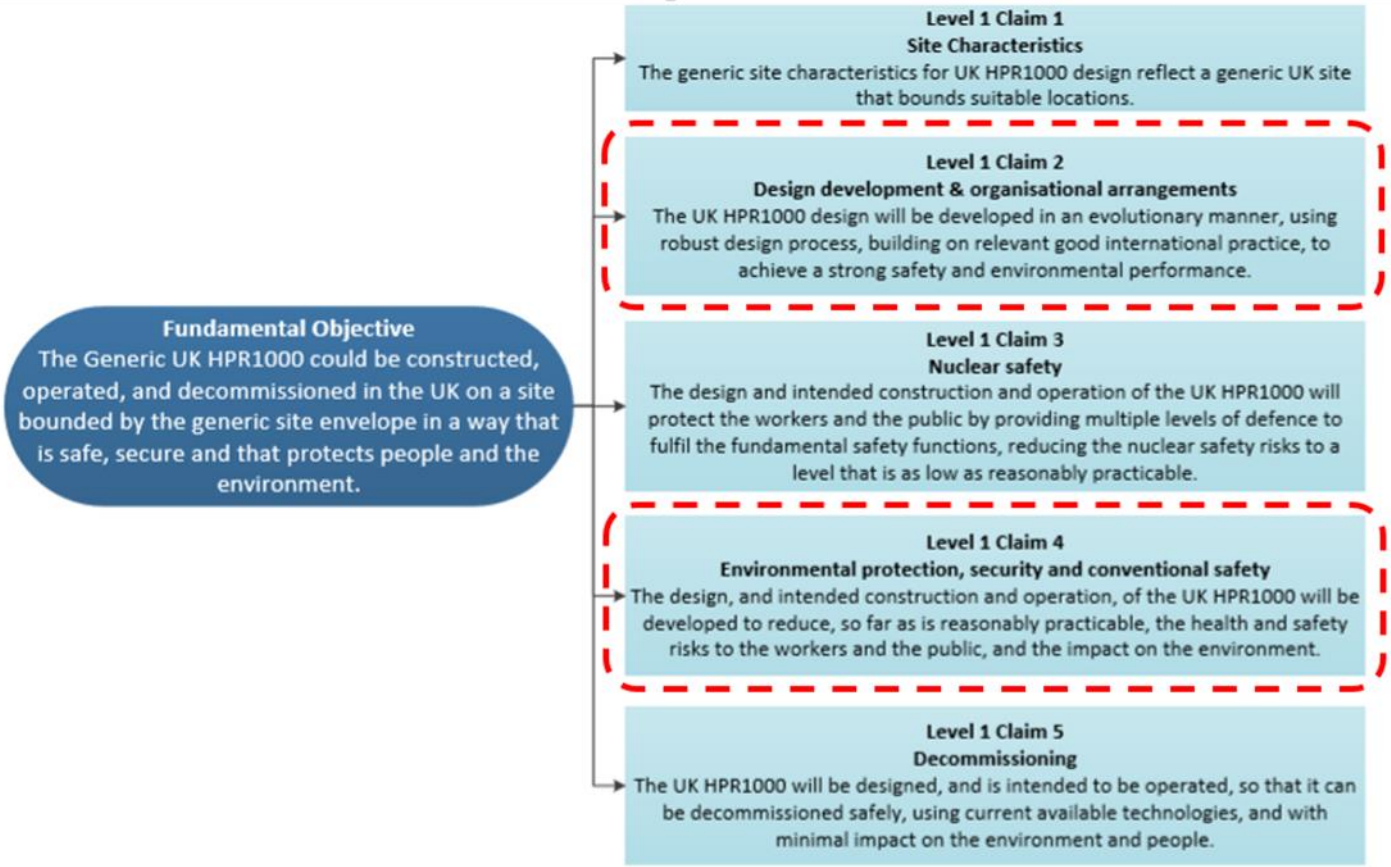
These claims, and their relationship to the fundamental objective, are highlighted in F 7.3-1.

F-7.3-2 shows the decomposition of Level 1 Claim 2 and highlights three further Level 2 claims of relevance to the GSR. These comprise:

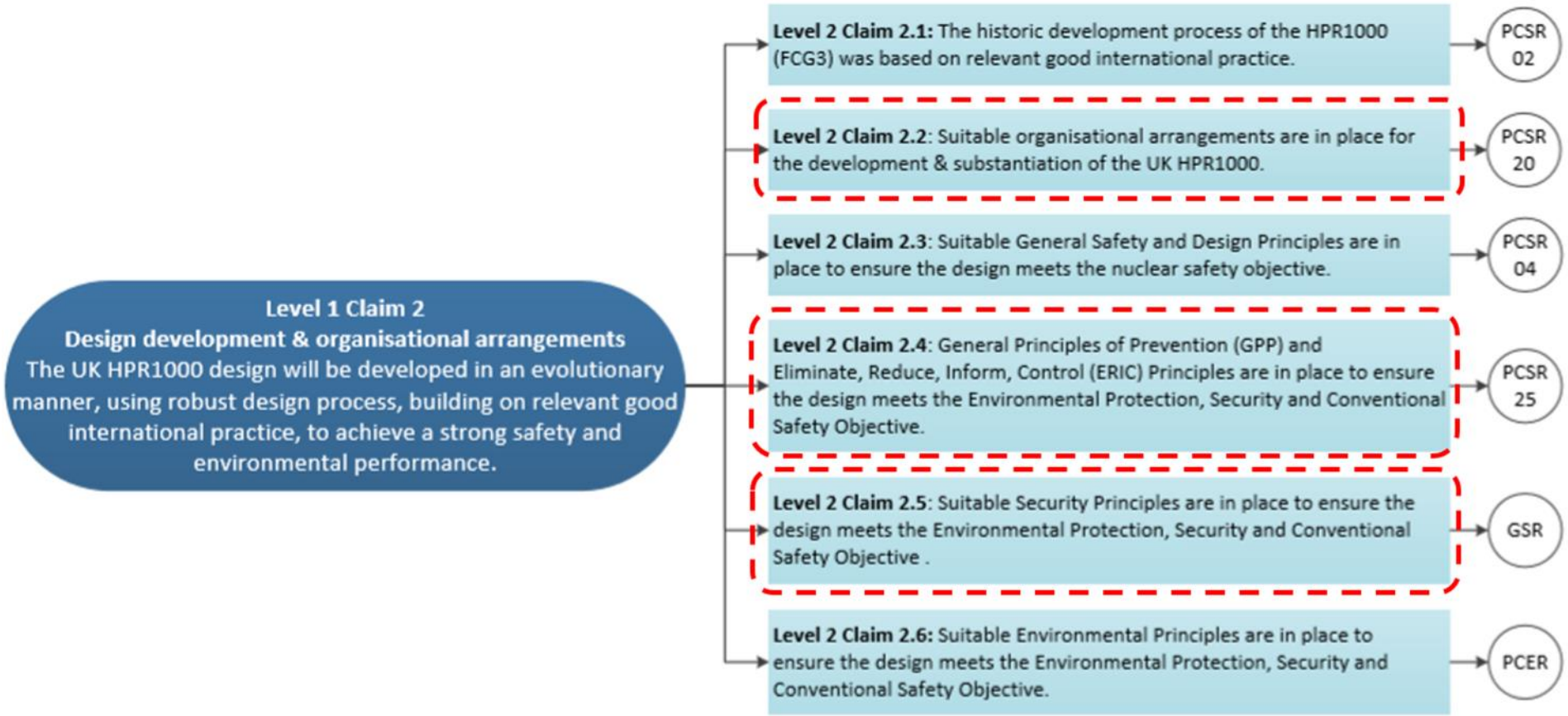
- Level 2 Claim 2.2 which requires suitable organisational arrangements are in place for the development of the UK HPR1000 and hence has relevance for the GSR and the security management system used in its production.
- Level 2 Claim 2.4, which discusses general principles of protection, and therefore has relevance to the GSR and associated developments including the application of the 'secure by design' principle.
- Level 2 Claim 2.5 which specifically relates to security principles.

Level 1 Claim 4 is presented in F-7.3-3. Of the subsidiary claims, Level 2 Claim 4.3 (highlighted in the Figure) is of relevance to the GSR as it specifically relates to the management of security risk for the UK HPR1000.

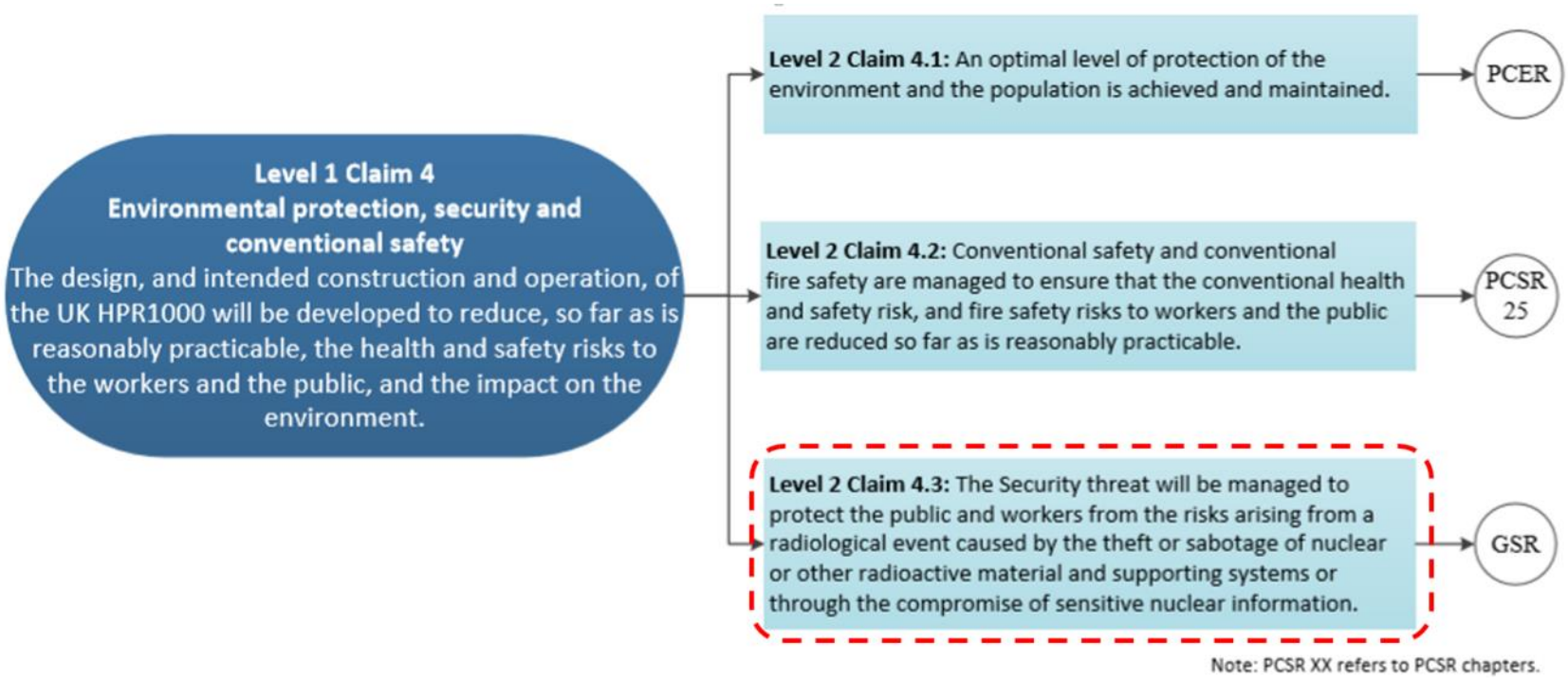
Hence, beneath each identified Level 2 Claim (comprising Claims 2.2, 2.4, 2.5 and 4.3) further sub-claims, arguments and evidence requirements have been developed. This CAE breakdown is presented in Annex A of this document and will subsequently be used within the proposed three tier GSR document (as presented in Section 8) structure to provide a clear and comprehensive route map through the documentation.




F-7.3-1 Fundamental Objective




F-7.3-2 Design Development and Organisational Arrangements



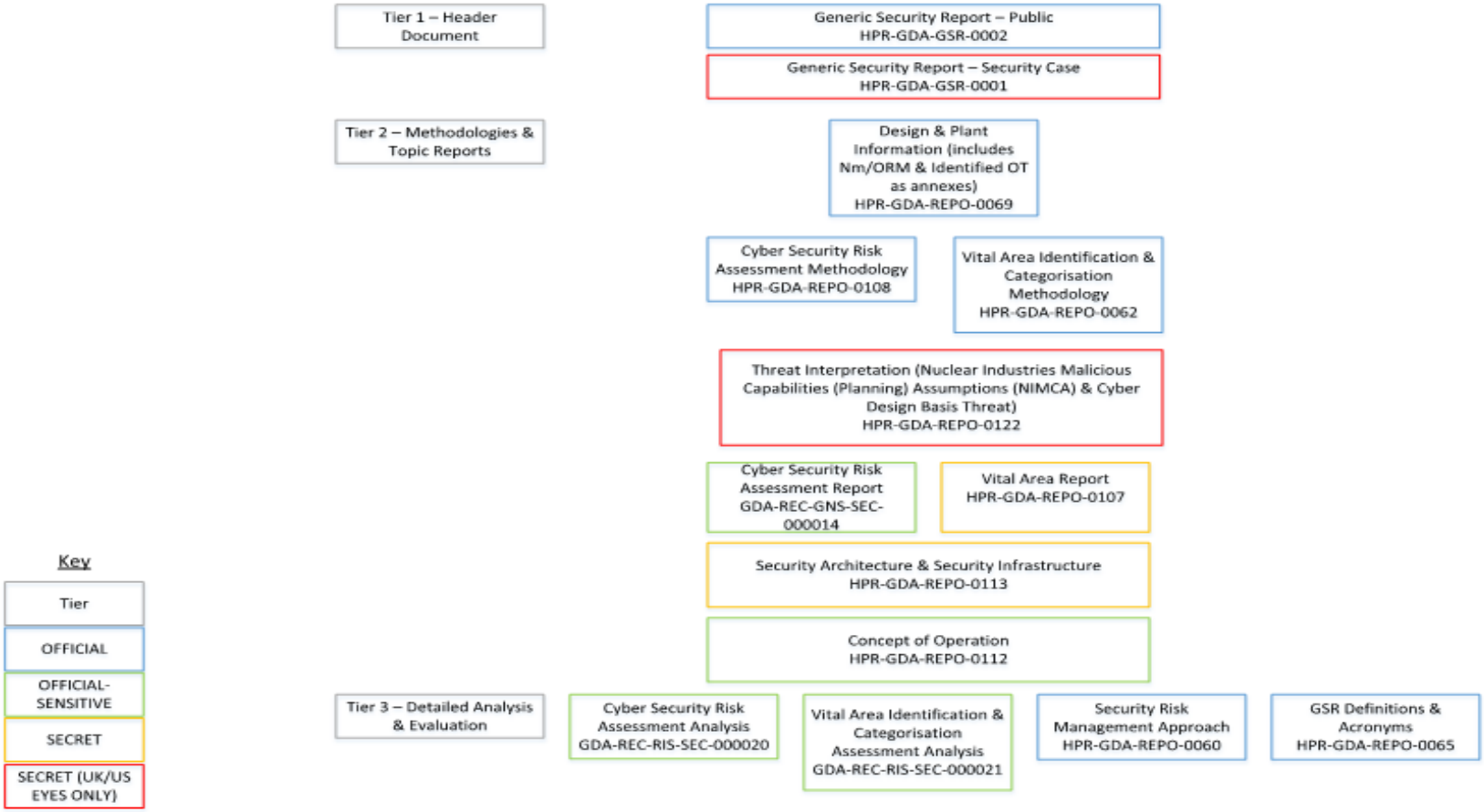

F-7.3-3 Environmental Protection, Security and Conventional Safety

# 8. Structure of the Generic Security Report

The GSR comprises a series of documents in three tiers as described below:

- Tier 1 – Security Report Head Document. This will lay out the security claims made by the GSR, summarise the Security Case from the detailed reports in Tier 2 below and provide the 'Golden Thread' through the hierarchy of GSR documents.
- Tier 2 – Documents which are directly referenced from the GSR. The documents describe the Methodologies that will be used in the detailed assessments in Tier 3, and provide detailed Topic Reports that draw on information from the Tier 3 assessments. These reports develop the security arguments that support the Tier 1 security claims.
- Tier 3 – Documents that use the methodologies from Tier 2 to conduct detailed assessments. These assessments provide the evidence to support the Tier 1 security claims and inform the Tier 2 reports.

Each tier contains one or more documents that support the tier above and the full series of documents is shown in F-8-1. The purpose of each document is summarised in the following sections.




F-8-1 Structure of the GSR

## 8.1 Tier 1 Head Documents

### 8.1.1 Generic Security Report – Security Case

The GSR-SC will be a classified, stand-alone head document at Tier 1 that will provide the security claims and references to the security arguments and evidence in the supporting Tier 2 and Tier 3 documents. The GSR will describe the security features of the proposed design, including the secure by design principle, and it will provide evidence that the security arrangements will meet regulatory expectations.

The key features of the GSR will be:

a) Methodologies to identify all targets within the NPP associated with the release of radiation to cause an Unacceptable Radiological Consequence (URC).

b) The categorisation of targets for theft or sabotage.

c) Analysis of cyber security risks for theft or sabotage.

d) Protective security outcomes within defined security postures.

e) Graded approach to Protective Security Measures (PSMs) to deliver defence in depth against the interpretation of the national DBT.

f) Security Categorisation and Classification of the PSMs.

g) Application of the 'Secure by Design' principle.

h) Clear trail of Claims, Arguments and Evidence to provide the 'Golden Thread' through the whole security case.

The GSR will also demonstrate that the production of the document has followed a robust process to show that:

a) The authors of each document are Suitably Qualified and Experienced Personnel (SQEP).

b) Quality Assurance Plan is in place to ensure that verification controls, approval procedures and independent reviews are conducted effectively.

The GSR will also capture assumptions, commitments and requirements as it is developed.

### 8.1.2 Generic Security Report – Public

The GSR-Public document will be a publicly-available version of the GSR-SC. To enable this, certain items of information will be redacted in the interests of national security.

## 8.2 Tier 2 Documents

### 8.2.1 Design and Plant Information (includes Nuclear Material/Other Radioactive Material and Identified Operational Technology)

The Design and Plant Information document is based on the Scope for UK HPR1000 GDA Project, Reference [6] and describes those elements of the NPP that will be assessed within the security case. It identifies the NPP buildings that are within scope and how the GSR will use information from both the PCSR and the PCER.

The document then gives more detailed descriptions of:

a) The site layout and main buildings.

b) Safety functions of, supporting systems and the interconnections between them.

c) Instrumentation and Control (I&C) systems (including Operational Technology (OT)).

d) Operating modes of the NPP.

e) Fuel route operations.

f) Radioactive waste management.

g) Inventory of NM/ORM.

The identification of key I&C systems and the inventory of NM/ORM are extremely significant, as they will be used as inputs into the Cyber Security Risk Assessment Analysis (Reference [8]) and the Vital Area Identification & Categorisation Assessment Analysis (Reference [9]).

### 8.2.2 Cyber Security Risk Assessment Methodology

This document details the methodology for the assessment of the risk of cyber intrusion and/or malicious action against Centralised I&C systems associated with the SSCs in the UK HPR1000 that could result in a URC. Furthermore, it will:

a) Define the threats to Computer Based Systems Important to Safety (CBSIS) and Computer Based Security Systems (CBSy).

b) Assess the level of cyber security risk against each system.

c) Identify system design features that affect security risk and potential security-based design improvements.

d) Determine the control sets to protect each system from the identified threats.

### 8.2.3 Vital Area Identification and Categorisation Methodology

This document describes the methodology used to identify and categorise VAs by following a five-phase process:

a) Identify NM/ORM with potential to cause an URC from the NM/ORM inventories document.

b) Identify combinations of SSCs that maintain the NM/ORM in a safe condition, which if compromised, could lead to a URC as potential targets.

c) Consider the physical and cyber threats identified in the Threat Interpretation document.

d) Identify credible threat acts that could compromise single or multiple targets to create a URC.

e) Identify and categorise VAs from credible threat acts to deliver proportionate security outcomes.

### 8.2.4 Threat Interpretation (Nuclear Industries Malicious Capabilities (Planning) Assumptions and Cyber Design Basis Threat)

This document presents the Physical and Cyber Security DBTs that apply to the UK HPR1000 Project within the GDA. The Physical Security DBT forms a direct interpretation of the threat assumptions from the NIMCA (Reference [10]), which defines the malicious capabilities associated with sabotage that need to be addressed in Vital Area Identification (VAI) studies for UK nuclear facilities.

The Cyber DBT is also derived from NIMCA (Reference [10]) and supplemented by information from publicly available sources, in a two-step process:

- A range of potential threat actors and supporting threat sources (intruders and insiders from the plant or supply chain) is identified from NIMCA (Reference [10]), applicable standards and other open source information.
- A review of the capability of the potential threat actors and supporting threat sources is carried out to identify potential means of affecting nuclear security and safety system operation to determine the associated cyber risks.

The publicly available sources for the Cyber DBT include:

- ONR's UK Civil Nuclear Sector, Cyber Threat Assessment (Reference [11]).
- HMG's 1A Standard Number 1 & 2, Information Risk Management (Reference [12]).
- HMG's 1A Standard Number 1 & 2 – Supplement, Technical Risk Assessment & Risk Treatment (Reference [13]).

### 8.2.5 Cyber Security Risk Assessment Report

The Cyber Security Risk Assessment Report describes the outcomes identified in the detailed analysis of the Cyber Security Risk Assessment Analysis Tier 3 activity. In particular, it will:

- Identify additional VAs to be protected.
- Identify cyber security control sets that will form an input into the Concept of Operations (CONOP) and Security Architecture / Security Infrastructure (SA/SI) process.
- Identify CBSIS that will need further security protection but will not lead to a URC if compromised.

### 8.2.6 Vital Area Report

The Vital Area Report presents the categorised VAs for the UK HPR1000 that have been identified through the Vital Area Identification & Categorisation Assessment Analysis. The VAs will be presented in building plot plans.

The report will also identify further areas within the UK HPR1000 design that will require protection that are outside of VAs (e.g. rooms containing CBSIS that are important but not critical).

### 8.2.7 Security Architecture and Security Infrastructure

The document takes the outputs from the Cyber Security Risk Assessment Report and the Vital Area Report to support the development of the generic security arrangements to protect the UK HPR1000 VAs.

The arrangements will provide proportionate security that will:

a) Deliver a defence in depth security regime.

b) Meet the required Physical Protection System (PPS) outcomes under SyAPs.

c) Meet the required Cyber Protection System (CPS) outcomes under SyAPs.

d) Protect NM/ORM from theft or sabotage.

The Security Architecture will describe the network architecture that will be required to support the security arrangements.

The Security Infrastructure will describe the arrangements themselves and indicative volumes of space that will be required (e.g. search areas; turnstiles).

High level details of CBSy will be provided.

Power and standby power requirements will also be described.

Deconflictions between security and safety requirements will be addressed.

Service connections between buildings will be reviewed.

#### 8.2.8 Concept of Operation

The document will describe a high level concept of how the security architecture and security infrastructure will be operated to provide defence in depth. In particular, it will describe the concepts behind:

a) A Site Security Control Room and alternate facility.

b) The provision of power and standby power to security systems.

c) The control sets to be applied from the cyber security risk assessment.

This will be used as a future framework for the SL to develop its NSSP.

### 8.3 Tier 3 Documents

#### 8.3.1 Cyber Security Risk Assessment Analysis

This document will provide the detailed assessment of the cyber security risks faced by CBSIS; CBSy will be assessed at a higher level due to uncertainties of system selection.

The assessment will use the Cyber Security Risk Assessment Methodology document and the cyber DBT from the Threat Interpretation document.

The results will be reported in the Cyber Security Risk Assessment Report.

It will:

a) Determine consequences of CBSIS system failure due to sabotage and determine CPS outcomes.

b) Assess CBSIS systems for design features that affect cyber security and identify potential security-based design changes.

c) Assess cyber security risks based upon threat actors / threat sources, CBSIS failure consequences and system design features.

d) Identify control Sets to be applied by the future SL in the CONOPs.

e) Identify additional VAs to be included in the VA Identification Assessment.

f) Determine the acceptability of cyber security risk and determine if the CPS outcomes have been achieved.

#### 8.3.2 Vital Area Identification and Categorisation Assessment Analysis

This document will provide the detailed assessment to identify and categorise VAs for

the UK HPR1000.

The assessment will use the Vital Area and Categorisation Methodology document and the physical threat from the Threat Interpretation document.

The results will be reported in the Categorised Vital Area Identification report.

It will identify:

a) Candidate targets.

b) Compromise activities.

c) Credible threat acts to create a URC.

d) Locations of VAs.

e) Categorisation of VAs.

### 8.3.3 Security Risk Management Approach

Security Risk Management Approach will describe an approach for managing security risks that could be adopted by the Licensee.

### 8.3.4 Generic Security Report Definitions and Acronyms

This document will provide security and safety case terminology, and acronym definitions, in support of the GSR report and supporting references.

# 9. Design and Plant Information

This section will describe the Design and Plant Information for the UK HPR1000. Key elements that are important to the security assessment of the UK HPR1000 for GDA include:

a) Site layout and main buildings – to identify the generic layout of the site and those buildings that will be included in the security assessment.

b) Properties of the civil structures in GDA scope – to describe the properties of the main buildings that will be considered during the assessment against the DBT.

c) Operating modes of the UK HPR1000 – to understand the different plant operating states and consider the combinations of SSCs that will be required to maintain the NM/ORM in a safe condition.

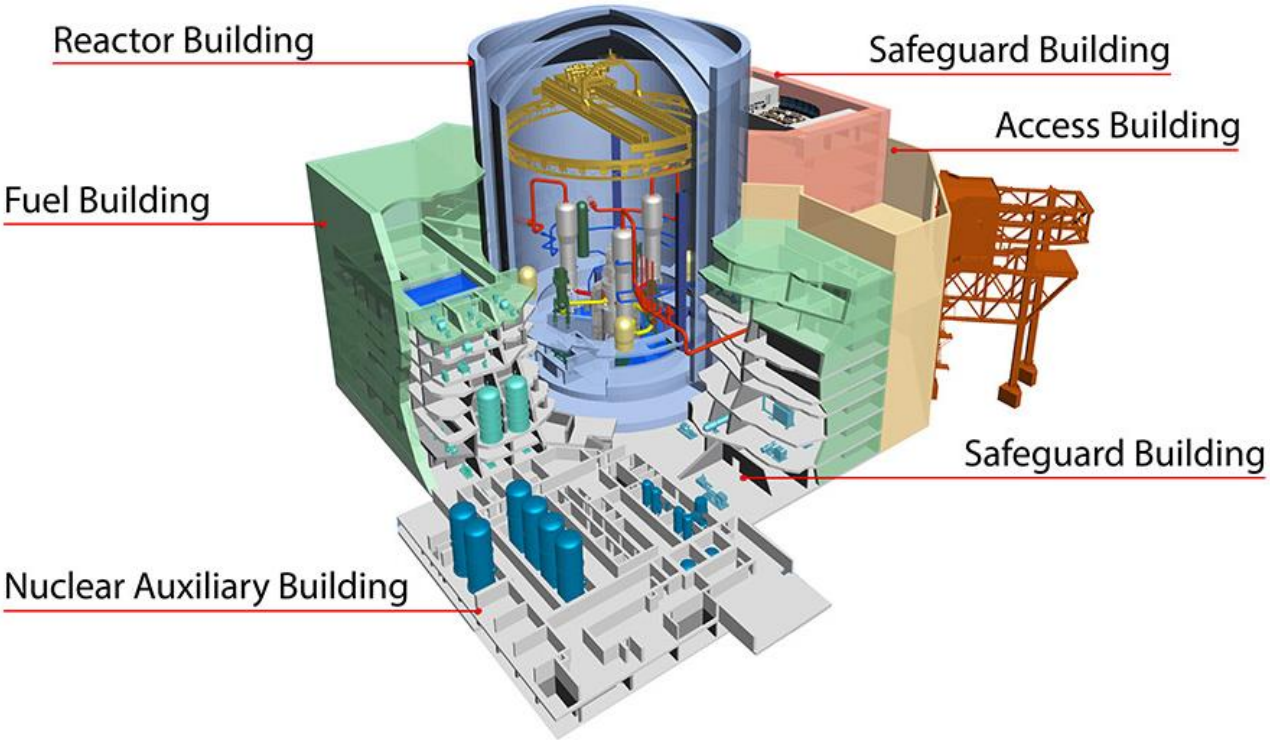
d) Fundamental Safety Functions – to understand the fundamental safety functions that are needed in order to maintain the NM/ORM in a safe condition.

e) Summary of the I&C and plant systems – to identify the SSCs that will deliver the Fundamental Safety Functions.

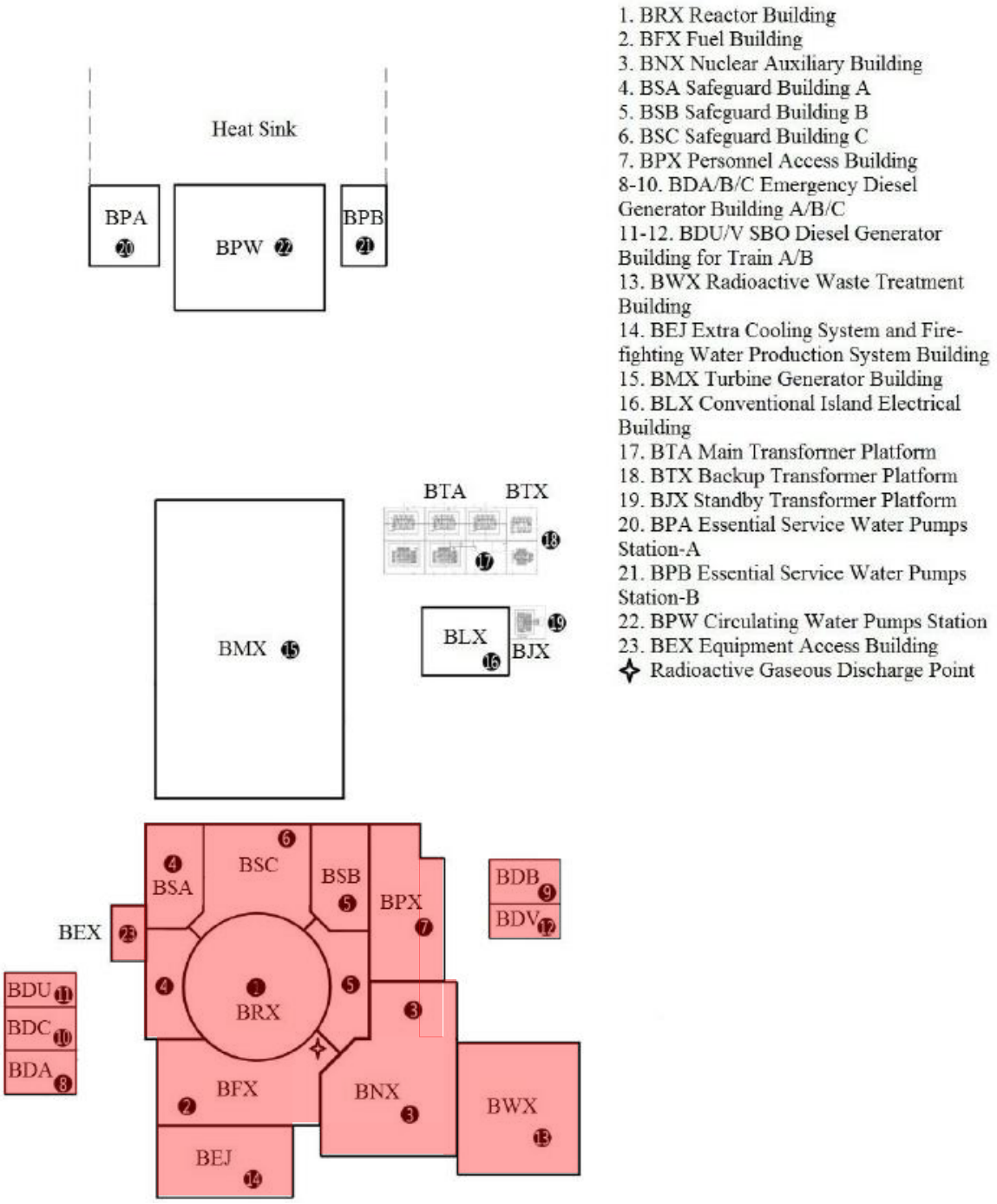
f) Inventory of NM/ORM with the potential to cause a URC – to identify the material that will need to be protected from theft or sabotage.

## 9.1 Site Layout and Main Buildings

The general layout of key buildings is presented in F-9.1-1 below, noting that the detailed layout of site buildings, especially those associated with Balance of Plant, will depend on site-specific characteristics. A plan view of the generic site layout is presented in F-9.1-2, and the key buildings within the scope of the GDA, extracted from Reference [6], have been shaded for clarity.




F-9.1-1 General Layout of UK HPR1000




F-9.1-2 Plan View of UK HPR1000 for GDA

T-9.1-1 below lists the buildings identified within the scope of the GDA (Reference [6]).

T-9.1-1 Buildings within UK HPR1000 GDA Scope

| No. | Building Code | Building Description |
|---|---|---|
| 1 | BDA | Emergency Diesel Generator Building A |
| 2 | BDB | Emergency Diesel Generator Building B |
| 3 | BDC | Emergency Diesel Generator Building C |
| 4 | BDU | SBO Diesel Generator Building for Train A |
| 5 | BDV | SBO Diesel Generator Building for Train B |
| 6 | BEX | Equipment Access Building |
| 7 | BFX | Fuel Building |
| 8 | BNX | Nuclear Auxiliary Building |
| 9 | BPX | Personnel Access Building |
| 10 | BRX | Reactor Building |
| 11 | BSA | Safeguard Building A |
| 12 | BSB | Safeguard Building B |
| 13 | BSC | Safeguard Building C |
| 14 | BWX | Radioactive Waste Treatment Building |
| 15 | BEJ | Extra Cooling System and Fire Fighting System Building |

## 9.2 Properties of Civil Structures in Generic Design Assessment Scope

Key dimensions and properties of the civil structures within the GDA scope are presented in T-9.2-1.

These properties will inform the Vital Area Identification & Categorisation Assessment

Analysis document as part of the assessment of the Physical DBT capabilities.

It is also notable that the BRX has been specifically designed to provide double containment for the extra protection of NM/ORM.

T-9.2-1 Properties of Civil Structures in GDA Scope

*T-9.2-1 has been redacted as it contains sensitive information*

## 9.3 Operating Modes

Normal operation of the HPR1000 includes six standard reactor operating modes, from full power operation to cold shutdown. These reactor modes are defined below:

a) Reactor in power (RP):

The reactor is either approaching critical or is critical, and is on the range of zero to full power operation. The reactor heat is transferred from the reactor core to the Steam Generators (SGs) in the secondary loop. The reactor coolant system is full and the pressuriser is in two-phase.

b) Normal Shutdown with Steam Generators (NS/SG):

The reactor is sub-critical. The residual heat from the reactor core is removed by the SGs. The residual heat removal system is isolated from the primary loop. Reactor coolant system is full and the pressuriser is in two-phase.

c) Normal Shutdown with RIS/RHR (NS/RIS-RHR):

The reactor is sub-critical. The residual heat removal system is connected to the primary loop. Reactor coolant system is full and the pressuriser is in single-phase or two-phase.

d) Maintenance Cold Shutdown (MCS):

The draining, air sweeping and maintenance of the reactor coolant system are performed in the MCS mode. The primary water level is higher than the minimum working water level of the residual heat removal system. The Reactor Pressure Vessel (RPV) head can be either closed or open in this mode

e) Refuelling Cold Shutdown (RCS):

The RPV head is removed. The primary loop is connected with the reactor pool. Refuelling activities are performed in this mode

f) Reactor Completely Discharged (RCD):

All the fuel assemblies are moved from the reactor core to the Fuel Building (BFX)

The safety assessment domains used in the Fault Analysis (i.e. Section 12 of the PCSR) are summarised in T-9.3-1 below.

T-9.3-1 Safety Assessment Domains

| Domain | Description |
|---|---|
| State A | Power States, Hot and Intermediate Shutdown States |
| State B | Intermediate Shutdown with temperature above $140^0$C |
| State C | Intermediate Shutdown and Cold Shutdown Conditions when RIS [SIS] is under RHR Operation Mode |
| State D | Cold shutdown with RCP [RCS] open |
| State E | Cold Shutdown During Refuelling |
| State F | Cold Shutdown when the Fuel Fully Unloaded |

These operating modes will be used by the analyses of the Cyber Security Risk Assessment and Vital Area Identification & Categorisation Assessment Analysis to identify SSCs, CBSIS and I&C systems that will require security protection.

## 9.4 Fundamental Safety Functions

Of particular importance to nuclear security are the safety systems associated with the delivery of the Fundamental Safety Functions (FSFs) for the plant for all plant operating modes.

Three FSFs are defined for the UK HPR1000 (Reference [2]):

a) R: Control of Reactivity (including prevention of accidental criticality)

b) H: Removal of Heat from the reactor and from the fuel store

c) C: Confinement of Radioactive Material, shielding against radiation and control of planned radioactive releases, as well as limitation of accidental radioactive releases

These three FSFs are decomposed into high level safety functions, as outlined below:

a) Control of Reactivity:

   1) R1: maintain core reactivity control

   2) R2: shutdown and maintain core sub-criticality

   3) R3: Prevention of uncontrolled positive reactivity insertion into the core

   4) R4: Maintain sufficient sub-criticality of fissile material stored outside the reactor coolant system but within the site

b) Removal of Heat:

1) H1: Maintain sufficient Reactor Coolant System water inventory for core cooling

2) H2: Remove heat from the core to the reactor coolant

3) H3: Transfer heat from the reactor coolant to the ultimate heat sink

4) H4: Maintain heat removal from radioactive material (including Spent Fuel, SF) with decay heat stored outside the reactor coolant system but within the site

c) Confinement:

1) C1: Maintain integrity of the fuel cladding

2) C2: Maintain integrity of the Reactor Coolant Pressure Boundary

3) C3: Maintain integrity of reactor containment

4) C4: Maintain integrity of fuel stored outside of reactor containment

5) C5: Store radioactive material

d) Extra Safety Functions:

1) E1: Support type R, H or C safety function

2) E2: Prevent, protect and mitigate hazards impact

The Fundamental Safety Functions (FSFs) will be used in the identification of Initiating Events of Malicious Origin (IEMOs) in the Vital Area Identification & Categorisation Assessment Analysis at Section 11 of this report. IEMOs are initiating events that could lead to a URC, and are caused deliberately (i.e. maliciously), and will be described in further detail in the later section.

### 9.5 Summary of the Instrumentation & Control and Plant Systems

This section identifies the SSCs that will deliver the FSFs to maintain the NM/ORM in a safe condition. Within the SSCs are I&C systems, to support the functions of the SSCs themselves. The criteria of overall I&C architecture are mainly derived from IAEA SSG-39, including single failure criterion, redundancy, independence, diversity, fail-safe, testability and maintainability, human factors and, importantly from a security perspective, cyber security. It is important for the GSR to recognise these criteria so that credit can be taken from designs within the Safety Case, and these will be explored further in the Cyber Security Risk Assessment section.

There are two groups of systems within I&C: those that have been identified as CBSIS and those that have not. Those systems identified as CBSIS have been further

subdivided into those that use computer-based technology (Centralised I&C Systems) to deliver the safety function of the system and those which use embedded technology (Smart Devices) (other I&C Systems) to deliver an aspect of the safety function.

Those systems that have been identified as CBSIS are highlighted and have been listed along with their locations in T-9.5-1 below.

T-9.5-1 List of CBSIS and Locations

| System | Description | Location |
|---|---|---|
| **Centralised I&C Systems** | | |
| RPR [RPS] | Reactor Protection System | Safeguard Building (BSA/B/C) |
| SAS | Safety Automation System | Safeguard Building (BSA/B/C) |
| PAMS | Post-Accident Monitoring System | Safeguard Building (BSA/B/C) |
| PSAS | Plant Standard Automation System | Safeguard Building (BSA/B/C) |
| KDA [SA I&C] | Severe Accident I&C System | Safeguard Building (BSA/B/C) |
| KDS [DAS] | Diverse Actuation System | Safeguard Building (BSA/B/C) |
| **Other I&C Systems** | | |
| RIC [ICIS] | In-core Instrumentation System | Safeguard Building (BSA/B/C), BRX |
| RPN [NIS] | Nuclear Instrumentation System | Safeguard Building (BSA/B/C), BRX |
| KIC [PICS] | Plant Computer Information & Control System | Safeguard Building (BSC (MCR)), RSS |

T-9.5-1 List of CBSIS and Locations

| System | Description | Location |
|---|---|---|
| KRT [PRMS] | Plant Radiation Monitoring System | Safeguard Building (BSA/B/C) |
| RGL [RPICS]) | Rod Position Indication and Rod Control System | Safeguard Building (BSA/B/C) |
| KPR [RSS] | Remote Shutdown Station System | Safeguard Building (BSC (MCR)), RSS |

T-B-1 in Annex B presents a summary of the function and principal locations of plant systems considered to be within the GDA scope (as defined by Reference [6]).

## 9.6 Inventory of Nuclear Material/Other Radioactive Material

An inventory of NM/ORM has been developed, comprising the following information:

- Description
- Type (NM or ORM)
- Location
- Quantity
- Form
- Characteristics
- Variation during plant lifecycle

The full inventory, listed in Reference [14], provides a critical input into the categorisation of NM/ORM for theft (Section 10) and the Vital Area Identification & Categorisation assessment from sabotage (Section 11). Categorising the inventory is an essential step in order to develop proportionate and graded security measures.

# 10. Categorisation of Nuclear Inventory for Theft

The requirement to categorise the inventory of NM/ORM is outlined in Reference [1] through Security Delivery Principle (SyDP) 6.1:

- 'Dutyholders should undertake characterisation of their site and facilities in order to determine the categorisation for theft'.

The categorisation approach is based on the quantities and forms of all NM and ORM held or used at the site. The NM/ORM inventory also considers how the inventory will change over time and hence provides a robust basis for the initial assessment of theft categorisation, noting that this assessment will be reviewed and updated where necessary as further information becomes available at future Design Reviews and Design Reference Points within the GDA programme.

The categorisation of the inventory considers NM, Radioactive Sources and ORM and is explained in detail in the UK HPR1000 Categorisation for Theft document (Reference [15]).

## 10.1 Nuclear Material

The NM/ORM inventory (presented in Reference [14]) confirms that the only material on site which constitutes NM are the fuel assemblies. Hence, NM will be located within the following facilities (within GDA scope) for the UK HPR1000:

- BFX
- BRX

Based on Table 1 of Reference [1] Annex A, the NM within the plant falls under the following Material Category:

- 'U235 in enriched uranium more than 0.711% U235 but *less than a greater percentage* unirradiated'

As each fuel assembly has a mass of Uranium below *a stated mass*, this material may be placed in a *low category*. This category applies to both unirradiated and irradiated fuel.

As the SF Cask system is likely to undergo modification for the UK design (for interim storage on-site), no proposal is made at this stage to apply a graded theft categorisation for fuel within the SF Cask.

## 10.2 Radioactive Sources

Although incomplete for UK HPR1000, radioactive sources are understood to be located in a number of buildings based on the NM/ORM inventory.

The source type, quantity and activity are not currently confirmed for the UK HPR1000. In addition, sealed sources for other purposes (e.g. instrument calibration or laboratory sources) will be located elsewhere within the site.

Reference [15] presents the provisional security groups for the radioactive sources used within the plant, based on the available data (Reference [14]) using Table 3 of Reference [1] Annex A.

As sources may be co-located in the same storage room or laboratory, consideration may need to be given to the effects of aggregation of the sources within a specific area.

### 10.3 Other Radioactive Material

ORM is present in the following in-scope buildings (based on NM/ORM inventory presented in Reference [14]):

- BFX
- BNX
- BRX
- BPX
- BWX

Some information is currently available for the ORM type, form and location however activity levels and nuclide composition data are not currently available. The information currently available is documented in Reference [14].

One sufficient data is available, categorisation for theft of ORM will be based on Table 4 of Reference [1] Annex A.

### 10.4 Conclusion

A review of the NM/ORM proposed to be located within the UK HPR1000 and the requirements of SyAPs Annex A, this section has concluded the following theft categorisations:

- Nuclear Material – *Low Category.*
- Radioactive Sources – source dependent, noting neutron sources not yet categorised.
- Other Radioactive Material – insufficient data at this stage to categorised.

The theft categorisations will be reviewed and updated as further data becomes available as the design continues to mature.

# 11. Vital Area Identification and Categorisation Methodology

To categorise NM/ORM for sabotage, it is necessary to identify Vital Areas (VAs) and then to categorise them according to the dose level of radiation that could be released over a specified period if sabotaged. This activity will be conducted over 2 stages: in the first stage, a VA Identification Methodology (VAIM) will be followed, in order to identify the VAs for the UK HPR1000; the second stage will then categorise the VAs according to the released dosage of radiation.

The identification of VAs for protection against sabotage and their subsequent categorisation is an essential part of the GSR. The definition of a VA is given in Annex B of Reference [1]:

> A VA is defined as, an area containing NM and/or ORM (including radioactive sources) or equipment, systems, structures or devices the sabotage or failure of which, alone or in combination, through malevolent acts as defined in the extant DBT, could directly or indirectly result in unacceptable radiological consequences, thereby endangering public health and safety by exposure to radiation.

The overall VAI process is two-fold and comprises:

(1) A five-phased approach to establish a set of categorised VAs for the UK HPR1000. See T-11-1.

(2) Regular reviews to examine the impact on the set of categorised VAs of subsequent changes to the:

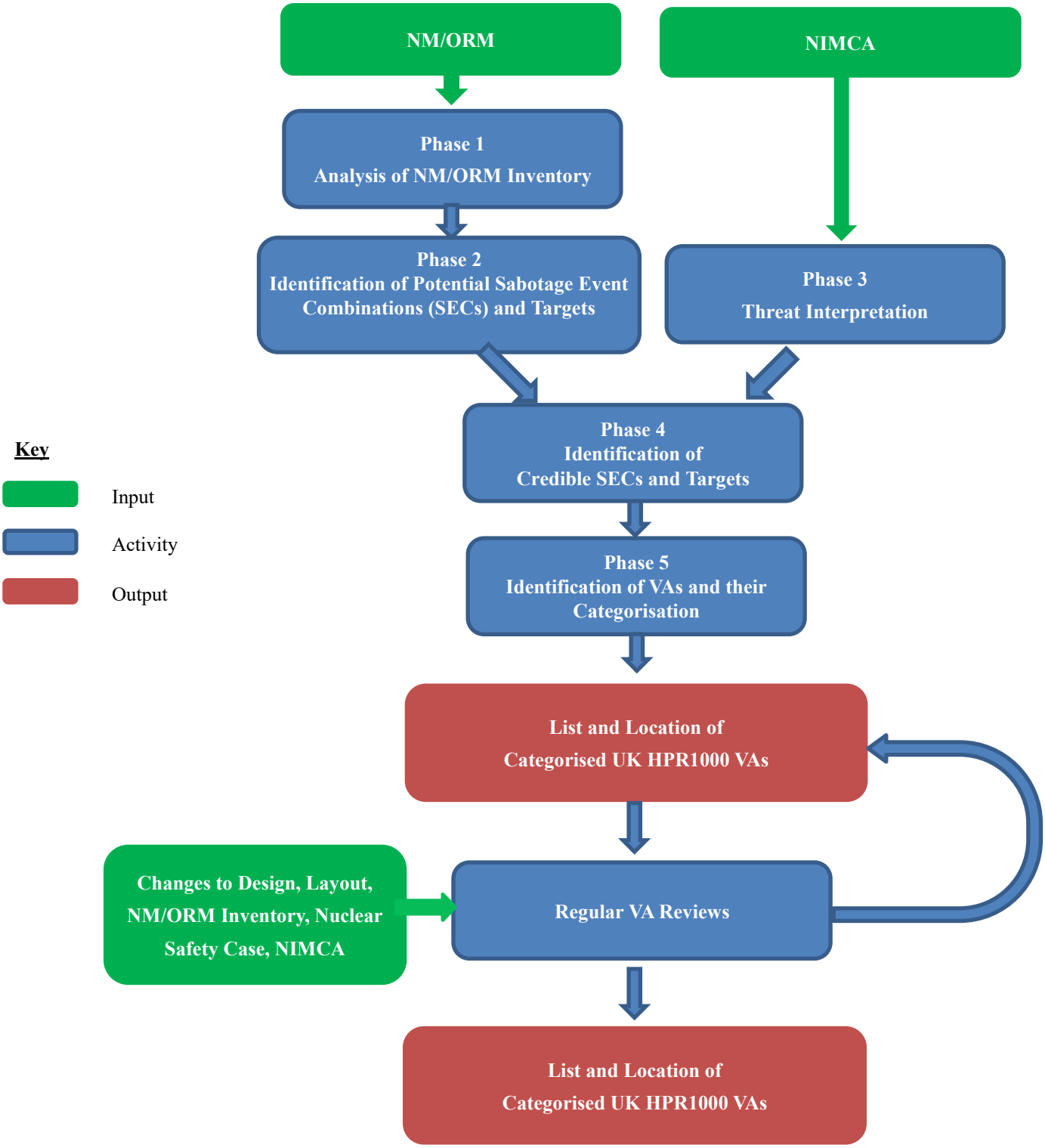
- Plant design and layout
- NM/ORM inventory
- PCSR
- NIMCA (Reference [10]).

A flow-chart of the overall VAI methodology for the establishment of the categorised UK HPR1000 VAs is given in F-11-1.

Details on the process adopted for each of the main activities shown in F-11-1 are presented in subsequent sections of this report, as tabulated below in T-11-1.

T-11-1 – Report Sections Containing Relevant VAI Methodology Phases

| | **Description** | **Section** |
|---|---|---|
| **Phase 1** | Analysis of NM/ORM Inventory | 11.1 |
| **Phase 2** | Identification of Sabotage Event Combinations (SECs) and Potential Targets | 11.2 |
| **Phase 3** | Threat Interpretation | 11.3 |
| **Phase 4** | Identification of Credible SECs and Credible Targets | 11.4 |
| **Phase 5** | Identification and Categorisation of VAs | 11.5 |
| **VA Review** | Regular VA Reviews | 11.6 |




F-11-1 Flow-chart for the VAIM of the UK HPR1000 VAs

## 11.1 Phase 1 – Analysis of Nuclear Material/Other Radioactive Material Inventory

The aim of Phase 1 is to identify the NM/ORM for the UK HPR1000 that requires

protection from sabotage.

The NM/ORM inventory from the Design and Plant Information document was developed and each source of NM/ORM was reviewed and its potential to cause a URC if unmitigated and unprotected was assessed.

A URC is defined in Annex B of Reference [1] as:

> An effective dose (including committed effective dose) of *more than a stated value* by all pathways over a *stated period of time* at the facility/transport package perimeter, to the most limiting member of the public, assuming a ground level release. This dose should be assessed on an unaverted basis (i.e. assuming no implementation of countermeasures during the *time period*), unless there are strong reasons for assessing the dose on an averted basis.

Any NM/ORM which was assessed as capable of delivering a URC was identified as requiring protection from sabotage. This assessment will also consider the bounding inventory at any point in the project lifecycle as well as proximity between adjacent NM/ORM sources.

The NM/ORM inventory was assessed for the potential to cause a URC if unmitigated and unprotected in the Vital Area Identification and Categorisation Assessment Analysis document (Reference [9]) and reported in the Vital Area Report (Reference [16]). T-11.1-1 below summarises the current inventory with the potential to cause a URC.

T-11.1-1 NM/ORM Inventory with Potential to Cause a URC

*T-11.1-1 has been redacted as it contains classified information.*

## 11.2 Phase 2 – Identification of Potential Sabotage Event Combinations and Potential Targets

The aims of Phase 2 are to identify the potential SECs and potential targets for protection against sabotage UK HPR1000.

For each source of NM/ORM that has been identified in Phase 1 as requiring protection from sabotage, the Phase 2 assessment comprises the following steps:

(1) The potential IEMOs which could challenge the FSFs keeping the source of NM/ORM in a safe state were identified via:

- The review of Postulated Initiating Events (PIEs) identified in Chapter 12 of the PCSR (Reference [2]).
- The review of PIEs excluded from safety case on a low frequency basis.
- Workshops with designers and operators of further events which could be

maliciously activated to challenge the safety of the plant.

(2) For each potential IEMO, the sequence of events that could lead to a URC was determined. This defines the SSCs and their combinations (where appropriate) which serve to prevent, protect or mitigate the loss of FSF potentially initiated by the IEMO. The IEMO and associated combination of SSCs become a potential SEC. The SSCs associated with the SEC become potential targets and where a potential target is a computerised system, then the associated CBSIS is identified and also included as potential targets.

(3) The potential SECs that could lead to a URC were reviewed to consider if any potential modifications could be made to the design which could eliminate or reduce the potential for the need for protection against sabotage. Such candidate design options were recorded and passed on to the plant modification process for consideration by the project. Should the design option be adopted by the project, then the SEC is discounted or reviewed and the reasons documented.

(4) Steps 1 to 3 were repeated for the different plant states and a complete list of UK HPR1000 potential SECs and targets for sabotage was produced.

The current assessment has identified a number of potential SECs for the UK HPR1000 as expected. These potential SECs, and the potential targets associated with each SEC, are shown in Annex C.

*Annex C has been redacted as it contains classified information.*

Initial assessment has shown that the list of potential IEMOs identified at Annex C will potentially compromise the following FSFs:

- Control of Reactivity:
  - R – Control of Reactivity (in general).
  - R4 – Maintain sufficient sub-criticality of fissile material stored outside the Reactor Coolant System (RCS) but within the site.
    - A further sub-set of R4 was identified and has been annotated as Fuel Route (FR). This sub-set has been applied to potential IEMOs that compromise R4 but specifically within the FR. These potential IEMOs have been identified as R4-FR in Annex C.
- Removal of Heat:
  - H1 – Maintain sufficient RCS water inventory for core cooling.
  - H2 – Remove heat from the core to the reactor coolant.
  - H3 – Transfer heat from the reactor coolant to the ultimate heat sink.

- H4 – Maintain heat removal from radioactive material (including SF) with decay heat stored outside the RCS but within site.

- Confinement:
  - C2 – Maintain integrity of the Reactor Coolant Pressure Boundary.
  - C4 – Maintain integrity of fuel stored outside of reactor containment.

The areas within the NPP that surround the potential targets that make up each potential SEC are termed Candidate VAs. The locations of the Candidate VAs for the potential SECs identified in the tables at Annex C are listed in Annex D.

*Annex D has been redacted as it contains classified information.*

### 11.3 Phase 3 – Threat Interpretation

The aim of Phase 3 is to derive the DBT for both physical and cyber security for use in the GDA of the UK HPR1000.

Phase 3 comprises two parallel activities to derive the DBT for the UK HPR1000 GDA, one focusing on the physical threat and the other on the cyber threat:

(1) The Physical DBT is derived from an interpretation of NIMCA (Reference [10]) which defines the malicious capabilities associated with sabotage.

(2) The Cyber DBT is derived from NIMCA (Reference [10]), supplemented by information from publicly available sources, in a two-step process:

- A range of potential threat actors and supporting threat sources (intruders and insiders from the plant or supply chain) is identified.
- The capabilities of the potential threat actors and supporting threat sources are reviewed to determine the associated cyber risks.

The interpretation of the applicable security threats to the UK HPR1000 from physical and cyber-attacks from the national DBT is contained in the Threat Interpretation document (Reference [17]) and shown in Annex E.

*Annex E has been redacted as it contains classified information.*

### 11.4 Phase 4 – Identification of Credible Sabotage Event Combinations and Credible Targets

The aim of Phase 4 is to identify the credible UK HPR1000 SECs and targets requiring protection from sabotage.

Phase 4 comprises the following steps:

(1) The capability required to prosecute each SEC identified in Phase 2 is assessed

relative to the GDA DBT capability derived in Phase 3 with the aim of:

- Identifying those SECs that can be credibly prosecuted by the DBT capability and hence requiring protection from sabotage.
- Eliminating from the VAI study those SECs that cannot be credibly prosecuted by the DBT capability.

(2) A review of the credible SECs is carried out to judge whether a design solution is available to eliminate the vulnerability. If so, then the proposed design modification is passed for further consideration by the General Nuclear System project team.

(3) A consolidated list of targets associated with each credible SEC is developed and their locations identified.

(4) Each identified target is reviewed and identified as:

- a direct target if the target can lead directly to a URC if sabotaged; or
- an indirect target if the target can only lead to a URC if sabotaged as part of an SEC containing multiple targets.

This Phase has not been completed for the UK HPR1000 and it will be conducted in the next revision of this document.

### 11.5 Phase 5 – Identification and Categorisation of Vital Areas

The aim of Phase 5 is to identify and categorise the UK HPR1000 VAs, within the scope of GDA.

Phase 5 comprises the following steps:

(1) The consolidated list and location of targets requiring protection from sabotage is first re-organised on a room by room basis, and all rooms containing a target are assigned as a VA.

(2) Each VA is then categorised as either a VA or a Higher Risk Vital Area. This categorisation is done as follows:

- If the sabotage of the targets within each room either on their own or as part of a SEC could lead to a URC with an offsite dose greater than *a stated value in a given time period* then the room is categorised as a Higher Risk Vital Area.
- If the sabotage of the targets within each room either on their own or as part of a SEC could lead to a URC with an offsite dose that is *between a lower and a higher value in given time period* then the room is categorised as a VA.

(3) The categorised VAs for the UK HPR1000 will be reported in both a tabular format and via plot plans. In order to inform the development of proportional and graded protection against sabotage, the following are denoted:

- VAs that contain at least one direct target are identified as a Direct VAs.
- VAs that only contain indirect targets are identified as Indirect VAs.

However, at this stage of GDA, no radiological consequence assessments are currently available which would allow refinement of the specific radiological dose attributable to the identified inventory with URC potential and, indeed, this is site specific information.

### 11.6 Vital Area Identification Reviews

To reflect developments in the UK HPR1000 design, layout, nuclear safety case and, if necessary, NIMCA during the GDA in the VAI process.

The five phases comprising the VAI process (as documented in Sections 11.1 to 11.5) are examined during every VAI review as appropriate and the associated output and documentation is revised to record the review.

The start point for the review is dependent on the development/change under consideration, e.g.

- A change to the nuclear inventory requires the VAI review to commence with the review of the impact of the change in Phase 1.
- A change to the PIEs requires the VAI review to commence with the review of the impact of the change in Phase 2.
- A change to NIMCA requires the VAI review to commence with the review of the impact of the change in Phase 3.

## 12. Cyber Security

Cyber security has a critical role to play in the protection of CBSIS, I&C, OT and Information Technology (IT) networks. The methodology to identify cyber security risks is described in the Cyber Security Risk Assessment Methodology (Reference [18]) and the detailed analysis is reported in the Cyber Security Risk Assessment Analysis document (Reference [8]). The outcomes from the analysis will be recorded in the Cyber Security Risk Assessment Report (Reference [19]), which is due for submission to ONR at the end of April 2020. This timetable for submission is reported in the Forward Action Plan at Section 17 of this report.

The Cyber Security Assessment Report will summarise the results of the analysis, as well as summarising the identified control sets to prevent or mitigate the effects of a cyber-attack, and any potential security-based design changes. It will also discuss other global cyber security issues such as the Insider threat, security in the supply chain and cyber risks that will exist post GDA.

The cyber security inputs that have been used within this version of the GSR have been drawn from the Cyber Security Risk Assessment Analysis. This analysis to date has reviewed the IEMOs and potential targets within the SECs to determine those containing CBSIS equipment that is potentially vulnerable to a cyber security threat. These potential CBSIS targets become inputs to Phase 2 of the VAIM, which is the Identification of Potential SECs and Targets with the potential to cause a URC.

The Cyber Security DBT for the UK HPR1000 has been identified in the Threat Interpretation (NIMCA & Cyber DBT) document (Reference [17]). The Threat Interpretation document has identified the threat actors and their capabilities, and forms part of the Threat Interpretation at Phase 3 of the VAIM. The Cyber Security DBT is further used in Phase 4 of the VAIM (Identification of Credible SECs and Targets) to create theft and sabotage scenarios to cause a URC. The scenarios will be developed in the next submission of the VA Report to ONR in the summer of 2020, and will consider pure cyber-attacks and also blended attacks, where physical and cyber-attack techniques will be combined.

The Cyber Security Risk Assessment Analysis has also begun a review of the design of each CBSIS system, in order to: determine design features that affect cyber security; define the consequence of single and multiple CBSIS system failure; and, perform the risk assessment for threat actor / threat source / sabotage event actions.

The Cyber Security Risk Assessment Analysis will also identify control sets that should be considered as preventative and mitigative protection measures against the cyber-attack. These control sets will be fed into the Security Architecture & Security Infrastructure document (Reference [20]) where they will be employed to support the delivery of the required Cyber Protection System outcomes, responses and functions to

provide evidence that the Regulator's security expectations within SyAPs will be met.

# 13. Security Architecture and Infrastructure

## 13.1 Introduction

This section presents the initial framework to identify the appropriate PSMs and layers that will be required to deliver proportionate security and achieve the principle of defence in depth across the NPP. The layers of PSMs will be identified under Security Architecture (SA) and Security Infrastructure (SI) to ensure that a complete security solution will be delivered.

## 13.2 Purpose

This section will describe the framework that will be used to develop proportionate physical and cyber PSMs to provide defence in depth to the protection of NM/ORM from theft or sabotage, and VAs, CBSIS and CBSy from sabotage.

## 13.3 Scope

The scope of assessment will include all buildings and facilities that have been identified in the Scope for UK HPR1000 GDA Project (Reference [6]) and described in the Design and Plant Information document (Reference [14]). This section will acknowledge, but not take credit for, PSMs that lie outside the GDA scope.

## 13.4 Definitions

The following definitions will be used:

### 13.4.1 Security Architecture

Security Architecture (SA) is defined as the high-level design of the integrated security system, which identifies the separate elements that collectively form the security infrastructure, and describes how the elements combine to deliver proportionate defence in depth and the required security outcomes. The design of the integrated security system (including physical and computer-based systems) will aim to:

- Disrupt or prevent events from occurring;
- Harden the system against initial compromise;
- Simplify the detection of a compromise;
- Limit the impact of any compromise;
- Harden the system against disruption;
- Be independent of other systems;
- Provide defence in depth;

- Support recovery.

### 13.4.2 Security Infrastructure

Security Infrastructure (SI) is defined as the layers of PSMs (PPS and CPS) required to deliver a security solution with defence in depth. The PSMs will be proportionate and provide a balance between the operability and security of the NPP, whilst meeting the UK's regulatory requirements for civil nuclear security.

## 13.5 Relevant Good Practice

The approach to identifying the SA and SI for the protection of the NPP is consistent with Relevant Good Practice (RGP) including:

1. Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities, International Atomic Energy Agency INFCIRC/225/Revision 5;
2. Security Assessment Principles (SyAPs) for the Civil Nuclear Industry 2017 Edition, Version 0;
3. ONR Nuclear Security Technical Assessment Guides – series;
4. Previous GDA Security Reports – notably the Conceptual Security Arrangements for the UK Advanced Boiling Water Reactor.

   The approach has also been informed by relevant international experience.

## 13.6 Regulatory Framework

### 13.6.1 Assessment Principles

Under the current regulatory framework, the GSR must provide evidence that the PSMs for the NPP, identified by the SA and SI, will provide outcomes to satisfy the requirements of SyAPs (Reference [1]). SyAPs identifies these requirements under FSyPs, SyDPs and Key Security Plan Principles (KSyPPs). This section presents those principles that are relevant to the development of the SA and SI by the RP for GDA purposes only. The principles that are relevant to the RP are shown in T-13.6-1 below.

T-13.6-1 SyAPs Relevant to the Development of SA and SI by the RP

| SyAP | Description |
|---|---|
| FSyP 5 – Reliability, Resilience and Sustainability | |
| SyDP 5.1 | Reliability and Resilience |
| FSyP 6 – Physical Protection Systems | |

T-13.6-1 SyAPs Relevant to the Development of SA and SI by the RP

| SyAP | Description |
|---|---|
| SyDP 6.1 | Categorisation for Theft |
| SyDP 6.2 | Categorisation for Sabotage |
| SyDP 6.3 | Physical Protection System Design |
| SyDP 6.4 | Vulnerability Assessments |
| FSyP 7 – Cyber Security and Information Assurance | |
| SyDP 7.1 | Effective Cyber and Information Risk Management |
| SyDP 7.2 | Information Security |
| SyDP 7.3 | Protection of Nuclear Technology and Operations |
| SyDP 7.4 | Physical Protection of Information |
| FSyP 10 – Emergency Preparedness and Response | |
| SyDP 10.1 | Counter Terrorism Measures, Emergency Preparedness and Response Planning |
| SyDP 10.3 | Clarity of Command, Control and Communications Arrangements During and Post a Nuclear Event |
| KSyPPs | |
| KSyPP 1 | Secure by Design |
| KSyPP 2 | The Threat |
| KSyPP 3 | The Graded Approach |
| KSyPP 4 | Defence in Depth |
| KSyPP 5 | Security Functional Categorisation and Classification |
| KSyPP 6 | Codes and Standards |

### 13.6.2 Security Outcomes and Responses

The SA and SI must also meet appropriate security outcomes and responses as determined by the category of NM or ORM from theft, or the classification of VA from sabotage, that is being protected.

### 13.6.3 Security Postures and Functions

Similarly, the SA and SI will support the CPS and PPS to deliver appropriate security postures against security functions to protect NM, ORM and VAs.

## 13.7 Protection Security Measures

### 13.7.1 Introduction to Approach

The PSMs identified as part of the SA and SI for the UK HPR1000 will deliver effective security measures to restrict access to areas across the NPP to those personnel with the appropriate levels of authorisation. This document will develop to identify appropriate PSMs, and show their locations, to prevent the theft or sabotage of key assets, across the NPP.

### 13.7.2 Aim

The aim of employing SA and SI is to prevent a URC by:

- Protecting NM/ORM from theft or sabotage;
- Protecting CBSIS and CBSy from sabotage;
- Protecting Sensitive Nuclear Information (SNI) from theft; and
- Preventing unauthorised access to VAs.

Access to NM, ORM, CBSIS, CBSy and VAs will be controlled through a series of protective layers.

### 13.7.3 Selection of Appropriate Cyber Protection Systems and Physical Protection Systems

In order to select appropriate CPS and PPS that will protect assets from theft and sabotage whilst allowing the NPP to operate, it is necessary to conduct an assessment across the site to: determine which assets need to be protected; identify where those assets are located; and, determine the appropriate levels of security to be applied.

A framework methodology will be used to ensure that sufficient levels of security will be applied, and any security vulnerabilities will be identified and eradicated. This methodology is described in the following section and provides the framework within which the SA and SI will be developed for the UK HPR1000. By following the methodology, and meeting the appropriate security requirements and functions as described in SyAPs, it will be possible to define the appropriate PSM types that will be adopted to deliver the correct levels of security to protect the relevant assets from theft or sabotage.

### 13.7.4 Generic Design Assessment Framework Security Architecture/Security Infrastructure Methodology to Assess and Identify Appropriate Protection Security Measures

The framework methodology for GDA is shown in F-13.7-1:

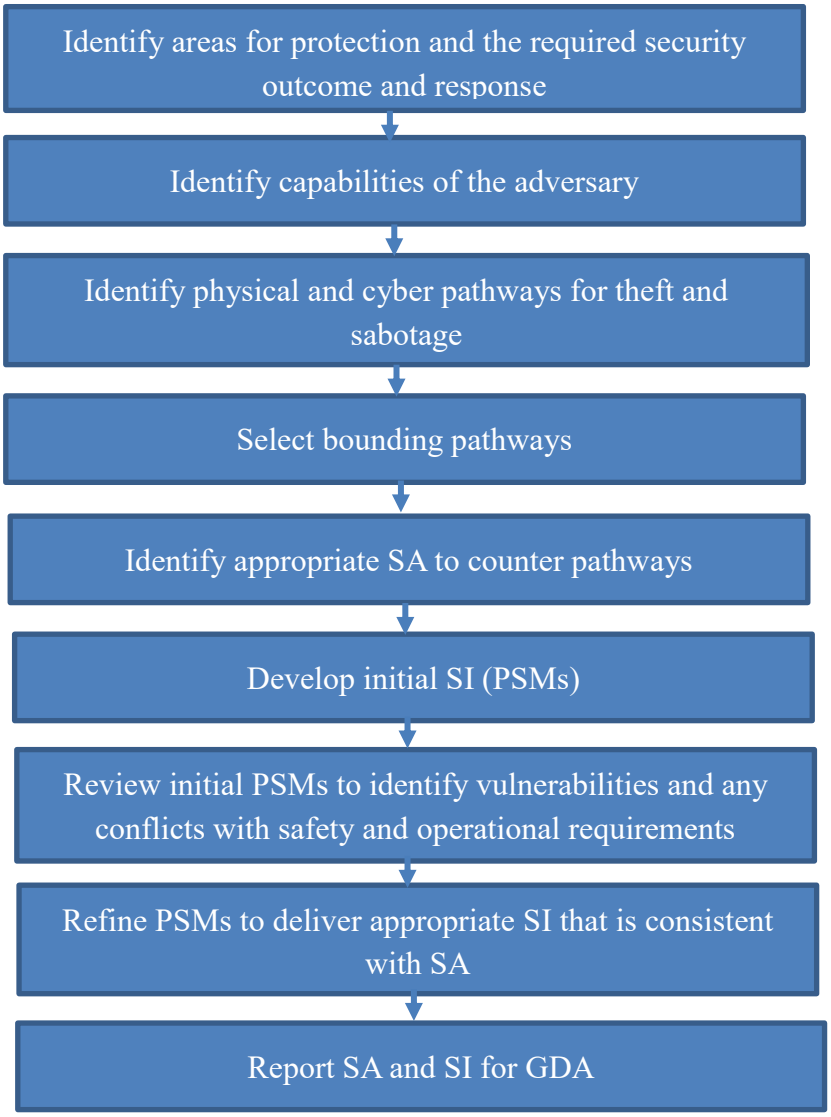



Figure F-13.7-1 GDA Framework SA/SI Methodology to Identify PSMs

The framework will be developed throughout the GDA to identify SI that will provide a conceptual, integrated security system to meet the design requirements of the SA.

## 13.8 Defence in Depth

The final outcome of the SA and SI assessment will be the design of an integrated security solution for the UK HPR1000 that satisfies the defence in depth principle

(KSyPP 4). This principle requires the protection of assets by using layers of mutually supporting security measures, such that if one layer is defeated, there are further layers of protection that remain intact. Each layer will present an independent PSM so that one common failure will not breach multiple layers of security.

The SA and SI report will also present claims that the principle of defence in depth has been achieved, with coherent and comprehensive arguments and evidence to substantiate the claims.

# 14. Concept of Operation

This section presents the framework to be followed in order to develop the appropriate Concept of Operation (CONOP) to deliver proportionate security through a layered approach that will achieve the principle of defence in depth across the NPP. The framework will be designed within the GDA project by the RP with an expectation that the CONOP will be developed further by the SL.

The current framework for the CONOP is shown in Annex F, and particular focus will be applied to the following elements:

- Control Room
- Power supplies to security systems
- Standby and emergency power supplies to security systems

## 14.1 Purpose

The UK HPR1000 Security Architecture/Security Infrastructure (SA/SI) section describes the appropriate layers of PSMs that will be needed to protect NM/ORM from theft and sabotage, and VAs, CBSIS and CBSy from sabotage. The purpose of this section is to describe the framework for a CONOP that will be required to deliver the protective layers successfully. Once fully developed, the CONOP will enable the delivery of an integrated security system that meets the defence in depth principle described in SyAPs (Reference [1]), under the Key Security Plan Principle 4 (Defence in Depth).

## 14.2 Scope

A number of the sections within the CONOP will be developed within the GDA by the RP and these sections will be expanded in further iterations of this document. These sections have been identified in the framework CONOP, at Annex F.

The remaining sections of the CONOP are the responsibility of the SL and these will be expanded by the appropriate party when the details of the site specific integrated security solution are known.

The scope of assessment of this section will include all buildings and facilities that have been identified in the Scope for UK HPR1000 GDA Project (Reference [4]), and described in the Design and Plant Information section, and the PSMs to be developed in the SA/SI report (Reference [20]). It will acknowledge, but not take credit for, PSMs that lie outside the GDA scope (e.g. perimeter fences, armed patrols and security response forces).

## 14.3 Relevant Good Practice

The approach to developing the CONOP for the protection of the NPP is consistent with RGP including:

1. Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities, International Atomic Energy Agency INFCIRC/225/Revision 5;
2. Security Assessment Principles (SyAPs) for the Civil Nuclear Industry 2017 Edition, Version 0;
3. ONR Nuclear Security Technical Assessment Guides – series;
4. Previous GDA Security Reports – notably the Conceptual Security Arrangements for the UK Advanced Boiling Water Reactor.

The approach has also been informed by relevant international experience.

## 14.4 Regulatory Framework

### 14.4.1 Assessment Principles

The GSR must provide evidence that the CONOP for the NPP will provide outcomes to satisfy the requirements of SyAPs, under FSyPs, SyDPs and KSyPPs. The framework for the CONOP will align each section with the relevant security principle and also identify the party responsible for the development of each Section.

# 15. Secure by Design

This section of the GSR will be developed as the Vital Area Identification & Categorisation Assessment Analysis matures in future iterations of this document. The principle of Secure by Design will be delivered within the following themes:

- Safety Claims with Security Implications
- Specific Security Design Changes

These themes will be developed in the sections below.

## 15.1 Safety Claims with Security Implications

Typical examples within this section will include:

- Safety claims made on I&C architecture, such as:
    - Single failure criterion.
    - Redundancy.
    - Independence.
    - Diversity.
    - Fail-safe.
    - Separation and Segregation.
    - Testability & Maintainability.
    - Human Factors.
- Safety claims made on infrastructure, such as:
    - Civil structures:
        - External and internal wall thickness.
        - Ground and floor slab thickness.
        - Roof thickness.
        - Radiation shielding.
        - Safety doors for over-pressure and flooding resistance.
        - Safety alarm systems.
        - Emergency lighting.
    - Operational and Maintenance Procedures:

- Supervisor Checks
- Independent Review of Design Changes.
- Defined Personnel Roles.
- Periodic Testing.
- Operator Procedures Relating to Plant Faults.

## 15.2 Specific Security Design Changes

The potential security issues in T-15.2-1 have been identified within the cyber risk assessment. These issues are to be considered by the design team for potential design change and by the physical security process for the potential assignment of additional physical security measures. Where appropriate, these issues will be raised as potential design changes in accordance with the General Nuclear System Modification Control Procedure (Reference [21]).

T-15.2-1 – Potential Cyber Security Issues

*The contents of T-15.2-1 have been redacted as they contain classified information.*

# 16. Assumptions, Commitments and Requirements

The list of assumptions, commitments and requirements will develop throughout the GDA process and will be passed onto the Licensee for further consideration.

The contents of this section will aid the Licensee to understand the bases on which the GSR was developed, the design information that was available at the time and any recognised gaps in knowledge. This will assist the Licensee to adopt the GSR and to develop it into the NSSP.

A preliminary list is provided below:

## 16.1 Assumptions

- This assessment is based on DR1 design information available at the time of writing.
- This assessment does not consider any actions taken by the state to mitigate threats where the state is the primary responsible party within NIMCA (Reference [10]).
- Licensee provided systems and processes are not included in this assessment.

## 16.2 Commitments

- SL will implement the identified security measures/control sets or alternatives.

## 16.3 Requirements

- Additional design and safety information from DRP/DR2, DR2.2 and DR3 (e.g. cable routing, evacuation routes, approved Fault Schedule etc.) is needed.

## 17. Forward Action Plan

It is recognised that the security assessment is not complete and that the GSR is based on the design information presented at Design Reference 1. To this end, there will be one further revision of the GSR-SC(P) at the end of the GDA, once all of the security assessment has been completed.

The degree of change within the listed documents above is not known at this stage, but each version will also take into account any design changes introduced at Design Review 2/Design Reference Point, Design Review 2.2 and Design Review 3.

## 18. Conclusion

The GSR has been written against the information made available under Design Reference 1 and has been restructured since the original issue of the GSR-SC as Version 0 in May 2019. It forms the foundation of the security assessment that will be completed in Step 4 of the GDA programme.

The document has described the structure of suite of supporting references from which the GSR draws its reference material. It has shown the RP's understanding of the NPP through its layout, identification of safety-critical SSCs, CBSIS and I&C systems, and, the NPP's modes of operation and FSFs. It has also identified the inventory of NM/ORM and categorised it against theft and sabotage.

A VAIM was presented, which used a physical and cyber-security DBT that was defined specifically for the UK HPR1000 to identify credible SECs and Targets and these were recognised as Vital Areas. The Vital Areas were categorised according to the level of radiological release that would ensue following an act of sabotage. However, a more detailed assessment of Vital Areas against DR2/DRP will be submitted to ONR in the summer of 2020.

A cyber security risk assessment methodology was created, which identified CBSIS and I&C systems that would need protection from cyber-attack. The control sets that will provide that level of protection will be the subject of further assessment, together with a full review of the vulnerability of critical safety systems to cyber-attack. This further assessment will be presented to ONR at the end of April 2020.

Similarly, the identification of appropriate PSMs and a high-level Concept of Operation will be developed at the beginning of Step 4, and the Tier 2 reference documents will be submitted to ONR in August 2020.

The RP recognises the level of further assessment that is required to complete the GSR – Security Case. It has provided a Forward Action Plan that has been agreed with the Regulator and it is anticipated that the Regulator has confidence in the RP to deliver a suitable security case on time in order to conduct a meaningful assessment.

## 19. References

[1] ONR, Security Assessment Principles for the Civil Nuclear Industry, Version 0, 2017.

[2] General Nuclear System, UK HPR1000 Pre-Construction Safety Report, GHX 00620 00X KPGB 02 GN, Revision C.

[3] General Nuclear System, UK HPR1000 Pre-Construction Environmental Report, GHX 00510 001 KPGB 02 GN, Revision C

[4] ONR, New Nuclear Power Plants: Generic Design Assessment Guidance to Requesting Parties, ONR-GDA-GD-006 Revision 0.

[5] ONR, New Nuclear Power Plants: Generic Design Assessment Technical Guidance, ONR-GDA-GD-007 Revision 0.

[6] General Nuclear System, Scope for UK HPR1000 GDA Project, HPR/GDA/REPO/0007 Rev 000.

[7] ONR, Guidance on the Security Assessment of Generic New Nuclear Reactor Designs, CNS-TAST-GD-11.1 Revision 0.

[8] General Nuclear System, Cyber Security Risk Assessment Analysis, GDA-REC-RIS-SEC-000020.

[9] General Nuclear System, Vital Area Identification and Categorisation Assessment Analysis, GDA-REC-RIS-SEC-000021.

[10] ONR, Nuclear Industries Malicious Capabilities (Planning) Assumptions, SB 5/2/4/3.

[11] ONR, UK Civil Nuclear Sector, Cyber Threat Assessment, 16674-1-ONR-Threat-Assessment-Report, Version 1.1, March 2018.

[12] HMG, 1A Standard Numbers 1&2. Information Risk Management, Issue 4.0, April 2012.

[13] HMG, 1A Standard Number 1&2. Supplement Technical Risk Assessment and Risk Treatment, Issue 1.0, April 2012.

[14] General Nuclear System, Design and Plant Information, HPR-GDA-REPO-0069.

[15] General Nuclear System, UK HPR1000 Categorisation for Theft, HPR-GDA-REPO-0105.

[16] General Nuclear System, Vital Area Report, HPR-GDA-REPO-0107.

[17] General Nuclear System, Threat Interpretation (NIMCA & Cyber Design Basis Threat), HPR-GDA-REPO-0122.

[18] General Nuclear System, Cyber Security Risk Assessment Methodology, HPR-GDA-REPO-0108.

[19] General Nuclear System, Cyber Security Risk Assessment Report, GDA-REC-GNS-SEC-000014.

[20] General Nuclear System, Security Architecture and Security Infrastructure, HPR-GDA-REPO-0113.

[21] General Nuclear System, UK HPR1000 Modification Control Procedure, HPR-

GDA-PROC-0053, Revision 001.

# Annex A Level 3 Security Claims, Arguments and Evidence

| *Claim* | *Sub-Claim* | *Argument* | *Links* | *Evidence* |
|---|---|---|---|---|
| **2.2 Suitable Organisational Arrangements are in place for the development and substantiation of the UK HPR1000** | | | | |
| 2.2.1<br>The security team has the necessary skills, knowledge, experience and organisational capability. | 2.2.1.1<br>Suitable security management arrangements are in place and have been communicated to all participants. | 2.2.1.1.1<br>The security management arrangements have been developed to satisfy the overall intent of FSyP 1, 2 and 3. | FSyP 1 | PCSR Ch. 20 (or develop analogous security section) |
| | 2.2.1.2<br>The implementation of the security management arrangements is being monitored, inspected, audited and reviewed at an agreed frequency, based on risk. Any corrective action required is being documented and closed. | 2.2.1.2.1<br>The GSR has been developed under an approved ISO9001 QA system and management procedures to ensure an appropriate review of security arrangements and assessment.<br><br>2.2.1.2.2<br>Independent review of security documentation and arrangements is provided by EDF. | FSyP 2 | General Nuclear System QA Procedure<br>General Nuclear System Management Plan<br>General Nuclear System Document Review Forms<br><br>EDF Independent Audit Plan |
| | 2.2.1.3<br>The security team has the necessary skills and experience for their roles within the project. | 2.2.1.3.1<br>A suitable competence management process has been developed and applied for personnel in security-related roles. | FSyP 3 | General Nuclear System SQEP Register |

| *Claim* | *Sub-Claim* | *Argument* | *Links* | *Evidence* |
|---|---|---|---|---|
| **2.4 General principles of Prevention (GPP) and Eliminate, Reduce, Inform[1], Control (ERIC) Principles are in place to ensure the design meets the Environmental Protection, Security and Conventional Safety Objective.** | | | | |
| 2.4.1<br>The UK HPR1000 security assessment has applied the GPP and ERIC principles to the design of the UK HPR1000. | 2.4.1.1<br>The UK HPR1000 has developed a layered and proportional security solution that incorporates defence-in-depth. | 2.4.1.1.1<br>Vital areas have been categorised based upon their security significance to support the development of proportional security arrangements.<br>2.4.1.1.2<br>Cyber security risks and applicable control sets have been evaluated via a proportionate risk based approach | FSyP7 | SA/SI, CONOPs<br>VAIM categorisation methodology<br>CSRAM/CSRA |
| | 2.4.1.2<br>The secure by design concept ensures that a security hierarchy of controls is implemented for the UK HPR1000. | 2.4.1.2.1<br>The security hierarchy has been applied throughout all phases of the development of the UK HPR1000.<br>2.4.1.2.2<br>The security hierarchy of controls prioritises the following (in this order); elimination, substitution, passive engineering, active engineering and operational. | | SA/SI, CONOPs |
| | 2.4.1.3<br>The security assessment has identified design modifications for the UK HPR1000 in accordance with the secure by design concept. | 2.4.1.3.1<br>See 4.3.5 | | |

[1] Note that in the ERIC principles more generally the 'I' usually means "isolate", not "inform"

| *Claim* | *Sub-Claim* | *Argument* | *Links* | *Evidence* |
|---|---|---|---|---|
| **2.5 Suitable security principles are in place to ensure the design meets the environmental protection, security and conventional safety objective** | | | | |
| 2.5.1<br>The GSR is being developed in accordance with UK requirements, standards and RGP. | 2.5.1.1<br>UK RGP has been used to develop appropriate assessment methodologies in support of the development of the GSR. | TBC | | |
| | 2.5.1.2<br>UK Requirements and applicable international standards have been used to develop appropriate assessment methodologies in support of the development of the GSR | TBC | | |

| *Claim* | *Sub-Claim* | *Argument* | *Links* | *Evidence* |
|---|---|---|---|---|
| **4.3 The security threat will be managed to protect the public and workers from the risks arising from a radiological event caused by the theft or sabotage of nuclear or other radioactive material and supporting systems or through the compromise of sensitive nuclear information.** | | | | |
| 4.3.1<br>The nuclear inventory of the plant requiring protection from sabotage and theft has been identified. | 4.3.1.1<br>A suitable nuclear inventory, comprising nuclear material and other radioactive material for the UK HPR1000 has been established. | 4.3.1.1.1<br>The nuclear inventory is based on currently available information for the UK HPR1000 design.<br>4.3.1.1.2<br>The nuclear inventory considers form, location, activity and quantity of the NM/ORM as well as potential changes during the project lifecycle. | | Design & Plant Information Report<br><br>Design & Plant Information Report |
| | 4.3.1.2<br>The nuclear inventory has been reviewed to establish those items in the inventory with the potential to give rise to Unacceptable Radiological Consequences (URC) if sabotaged. | 4.3.1.2.1<br>The assessment of the URC potential of NM/ORM has been undertaken on a conservative basis using available information.<br>4.3.1.2.2<br>Appropriate radiological dose levels for URC assessment have been applied. | | Tier 3 VA Report<br><br>Tier 3 VA Report |
| | 4.3.1.3<br>The nuclear inventory has been appropriately categorised for the purpose of identifying the requirements for protecting it from theft. | 4.3.1.3.1<br>The NM/ORM inventory has been categorised for theft purposes using appropriate criteria. | FSyP 6 | Theft Report |
| 4.3.2<br>Targets and their locations requiring protection against theft and/or sabotage have been identified and suitably categorised for security | 4.3.2.1<br>A structured methodology has been developed and applied in line with UK RGP for the identification of Vital Areas for the UK HPR1000. | 4.3.2.1.1<br>The VAIM presents a structured methodology for the identification and categorisation of vital areas based upon the location of NM/ORM inventory and supporting safety systems. | | VAIM |

| *Claim* | *Sub-Claim* | *Argument* | *Links* | *Evidence* |
|---|---|---|---|---|
| purposes. | 4.3.2.2<br>Assets (comprising NM/ORM with URC potential) together with the plant and equipment required to prevent, protect or mitigate their sabotage from unacceptable radiological consequences have been identified. | 4.3.2.2.1<br>Sabotage Event Combinations (comprising IEMOs and SSCs whose sabotage could lead to a URC) have been developed.<br>4.3.2.2.1<br>The cyber security risk assessment has been used to identify potential targets within OT. | FSyP 7 | VAIM |
| | 4.3.2.3<br>Vital Areas have been established based on the location of NM/ORM requiring protection from sabotage as well as the locations of plant and equipment which maintain the NM/ORM in a safe condition (critical SSCs). | 4.3.2.3.1<br>Location data for UK HPR1000 NM/ORM and SSCs has been obtained.<br>4.3.2.3.2<br>The location and categorisation of Vital Areas have been plotted on floor plans. | | VAR<br>VAR |
| | 4.3.2.4<br>Vital Areas have been suitably categorised and assessed to support the development of a proportional and graded security regime. | 4.3.2.4.1<br>Vital Areas have been categorised based on the magnitude of the potential URC.<br>4.3.2.4.2<br>Vital Areas have been distinguished depending on whether their sabotage can lead directly to a URC or only in combination with the sabotage of other Vital Areas. | FSyP6 | VAR<br>VAR |
| | 4.3.2.5<br>Areas of the plant requiring protection in addition to the established Vital Areas are identified. | 4.3.2.5.1<br>Additional locations requiring protection for the purpose of protection against cyber-attack or theft of NM/ORM have been identified. | FSyP7 | CSRA |
| 4.3.3<br>A suitable design basis threat has been established | 4.3.3.1<br>Appropriate source documentation has been used to | 4.3.3.1.1<br>Extant NIMCA documentation has been used to develop the design basis threat. | | Threat Interpretation Document |

| *Claim* | *Sub-Claim* | *Argument* | *Links* | *Evidence* |
|---|---|---|---|---|
| and applied. | establish the capability and capacity of the national threat. | | | |
| | 4.3.3.2<br>An appropriate level of cyber threat has been applied in the assessment of the UK HPR1000. | 4.3.2.2.1<br>Cyber security documentation has been used to develop the UK HPR1000 specific cyber security threat assessment. This threat assessment has been applied through a defined cyber risk assessment methodology. | FSyP7 | Threat Interpretation Document<br>CSRAM |
| | 4.3.3.3<br>The UK threat has been interpreted for application to the UK HPR1000 project. | 4.3.3.3.1<br>A suitable and bounding design basis threat has been developed for application to the assessment of the UK HPR1000. | | Threat Interpretation Document |
| | 4.3.3.4<br>The interpretation of the UK threat has been used to inform the security assessment. | 4.3.3.4.1<br>The Vital Areas have been confirmed through application of the design basis threat to identify those sabotage event combinations (SECs) which are within the capability and capacity of the applied threat | KSyPP2 | T2 VAR |
| 4.3.4<br>Protection against theft and sabotage has been achieved via a combination of proportional physical, cyber and procedural measures. | 4.3.4.1<br>A concept of security operations has been established to provide defence-in-depth, proportional security and an effective security culture. | 4.3.4.1.1<br>A hierarchy of protective security measures has been developed to deliver a layered approach with defence-in-depth.<br>4.3.4.1.2<br>The concept of operations describes how protective safety measures will be delivered.<br>4.3.4.1.3<br>The GSR will form a key input into the development of the NSSP by the future licensee without foreclosing options for the licensee to develop alternative approaches. | FSyP6 | SA/SI<br>Possible control sets from CSRA<br><br>CONOPs |
| 4.3.5<br>Security considerations have influenced the design of the | 4.3.5.1<br>Potential plant design changes have been identified and | 4.3.5.1.1<br>Potential design modifications have been identified during the security assessment of the | | GSR Sections 8, 10 & 14 |

| *Claim* | *Sub-Claim* | *Argument* | *Links* | *Evidence* |
|---|---|---|---|---|
| UK HPR1000. | considered to eliminate or reduce the potential for sabotage and/or theft of the nuclear inventory. | UK HPR1000.<br>4.3.5.1.2<br>The 'secure by design' concept has been applied when considering potential plant modifications identified by the security assessment.<br>4.3.5.1.3<br>Design changes have been reviewed and assessed using a suitable design change assessment process. | | GSR Sections 8, 10 & 14<br><br>General Nuclear System Modification Control procedure HPR-GDA-PROC-0053 Revision 001 + minutes from design review meeting |
| | 4.3.5.2<br>Potential design modifications have been considered for their security implications where relevant. | 4.3.5.2.1<br>Security considerations have been included in the assessment of potential plant design modifications for the UK HPR1000.<br>4.3.5.2.2<br>Security-related design modifications have been considered and assessed using a formal project process. | | GSR Section 8; part of security organisation structure under Claim 2.2 + design review meeting minutes that show security as an agenda item<br><br>General Nuclear System Modification Control procedure HPR-GDA-PROC-0053 Revision 001 + minutes from design review meeting |
| | 4.3.5.3<br>Aspects of the UK HPR1000 design and operations have been deconflicted where necessary. | 4.3.5.3.1<br>The UK HPR1000 design and operations has been reviewed from the security perspective (e.g. evacuations and invacuation routes, doors and barriers) with the assessment integrated nuclear safety, conventional safety and environmental safety aspects of the design. | | CONOPs |
| | 4.3.5.4<br>The UK HPR1000 includes adequate provision for the | 4.3.5.4.1<br>Appropriate space and infrastructure for security systems has been allowed for in the design of the | | SA/SI |

| *Claim* | *Sub-Claim* | *Argument* | *Links* | *Evidence* |
|---|---|---|---|---|
| | development of appropriate security measures. | UK HPR1000. | | |
| 4.3.6<br>Sensitive nuclear information will be subject to appropriate security controls. | 4.3.6.1<br>The CONOP highlights the future requirement for the Licensee to protect SNI. | - | FSyP7 | CONOPs<br>Licensee |

# Annex B Principal Locations of Plant Systems within Generic Design Assessment Scope

T-B-1 Summary of the Function and Principal Locations of Plant Systems Considered to be Within the GDA Scope

| No | System Code | System Description | Function(s) | Key Locations(s) |
|---|---|---|---|---|
| Critical Structures, Systems and Components | | | | |
| 1 | ADG [FDTGSS] | Feedwater Deaerating Tank and Gas Stripper System | Maintains feedwater quality | BMX |
| 2 | APG [SGBS] | Steam Generator Blowdown System | Maintains chemical characteristics of SG secondary water | BNX, BFX, BRX |
| 3 | ARE [MFFCS] | Main Feedwater System | Supplies feedwater to the secondary side of the SGs during normal operations | BRX, BSA/BSB/ BSC, BMX |
| 4 | ASG [EFWS] | Emergency Feedwater System | Supplies emergency feedwater to the SGs in the event of loss of ARE [MFS] to remove residual heat | BSA/BSB/ BSC |
| 5 | ASP [SPRHRS] | Secondary Passive Residual Heat Removal System | Backup means of removing decay heat (secondary side) via passive heat transfer | BRX |
| 6 | ATE [CPS] | Condensate Polishing System | Removes impurities of corrosion products from condensate to ensure feedwater and steam meet requirements | BMX |
| 7 | DEL [SCWS] | Safety Chilled Water System | Cooling water system providing heat sink to DVL, DWL, DWK and DCL. Three train system two are cooled by air, third by RRI | BSA/BSB/ BSC |

T-B-1 Summary of the Function and Principal Locations of Plant Systems Considered to be Within the GDA Scope

| No | System Code | System Description | Function(s) | Key Locations(s) |
|---|---|---|---|---|
| 8 | DFL [SCS] | Smoke Control System | Exhausts smoke from fire and protects the protected rescue routes against smoke ingress. | BSA/BSB/ BSC, BDX, BNX, BAX, BWX. BEJ, BFX, BPX |
| 9 | DMK [FBHES] | Fuel Building Handling Equipment System | All fuel handling equipment in BFX | BFX |
| 10 | DMR [RBHES] | Reactor Building Handling Equipment System | All fuel handling equipment in BRX | BRX |
| 11 | DVL [EDSBVS] | Electrical Division of Safeguard Building Ventilation System | Maintains ambient conditions (temperature, humidity and cleanliness) within the acceptable range for personnel and equipment in DVL | BSA/BSB/ BSC |
| 12 | ECS [ECS] | Extra Cooling System | Removes residual heat from SFP in event of loss of normal cooling (e.g. SBO, TLOCC) | BEJ, BFX, BSA/BSB |
| 13 | EDE [AVS] | Containment Annulus Ventilation System | Maintains negative pressure during normal operation of the annulus and enables the annulus to reach a negative pressure at the beginning of an accident. | BFX |

T-B-1 Summary of the Function and Principal Locations of Plant Systems Considered to be Within the GDA Scope

| No | System Code | System Description | Function(s) | Key Locations(s) |
|---|---|---|---|---|
| 14 | EHR [CHRS] | Containment Heat Removal System | Transfers residual heat from the containment to the ultimate heat sink under accident conditions. System includes the containment spraying subsystem, the reactor pit injection subsystem, the strainer back-flushing subsystem and the passive reactor pit injection subsystem. | BRX, BSA/BSB |
| 15 | EPP [CLRTMS] | Containment Leak Rate Testing and Monitoring System | Collects potential radioactivity release from containment under accident conditions, and contributes to the containment isolation and integrity. The EPP [CLRTMS] includes the leak recovery sub-system and containment leak tightness test sub-system. | BRX, BFX, BSA, BSB, BSC |
| 16 | EUF [CFES] | Containment Filtration and Exhaust System | Provides active pressure relief to lower containment pressure and protect containment integrity. | BFX, BRX |
| 17 | EUH [CCGCS] | Containment Combustible Gas Control System | Reduces the hydrogen concentration in containment during accident conditions | BRX |

T-B-1 Summary of the Function and Principal Locations of Plant Systems Considered to be Within the GDA Scope

| No | System Code | System Description | Function(s) | Key Locations(s) |
|---|---|---|---|---|
| 18 | EVF [CIFS] | Containment Internal Filtration System | Reduces the concentration of radioactive iodine and aerosol in containment during normal operations | BRX |
| 19 | EVR [CCVS] | Containment Cooling and Ventilation System | Maintains ambient conditions for staff and equipment in BRX | BRX |
| 20 | GCT [TBS] | Turbine Bypass System | Allows steam to be dumped to the condensers to remove decay heat | BMX |
| 21 | JAC [FWPS] | Fire-fighting Water Production System | Provision of water (two dedicated pools and three pumps) to NI fire-fighting systems | BEJ |
| 22 | JDT [FDCS] | Fire Detection and Control System | Detects the start of a fire and signals location to fire detection panels. | NI |
| 23 | JPI [NIFPS] | Nuclear Island Fire Protection System | Provides hydrant and fixed sprinkler systems for NI Buildings | NI Buildings |
| 24 | KCC [NEMS] | Nuclear Emergency Management System | Provides information and technical support for the on-site emergency management | OECC |

T-B-1 Summary of the Function and Principal Locations of Plant Systems Considered to be Within the GDA Scope

| No | System Code | System Description | Function(s) | Key Locations(s) |
|---|---|---|---|---|
| 25 | PTR [R&FPCTS] | Reactor pool and Fuel Pool Cooling and Treatment System | Provides cooling, purification, skimming, filling and draining for BRX pools (including reactor cavity and internals storage pool) and BFX pools (including SFP, fuel transfer compartment and cask loading pit), as well as providing shielding, cooling and criticality control for fuel handling and storage | BRX, BFX |
| 26 | RBS [EBS] | Emergency Boration System | Provides boration of the primary loop to compensate for reactivity changes during cooldown and emergency boration following ATWS events | BFX, BSC, BRX |
| 27 | RCP [RCS] | Reactor Coolant System | Reactor primary circuit; provides three loops, each with one SG, reactor coolant pump and main coolant line as well as one pressuriser | BRX |
| 28 | RCV [CVCS] | Chemical and Volume Control System | Provides reactor coolant volume control, reactivity control, chemical control and RCP [RCS] pump seal injection functions | BNX, BRX, BFX |

T-B-1 Summary of the Function and Principal Locations of Plant Systems Considered to be Within the GDA Scope

| No | System Code | System Description | Function(s) | Key Locations(s) |
|---|---|---|---|---|
| 29 | REA [RBWMS] | Reactor Boron and Water Makeup System | Makes up boric acid solution or demineralised water to RCP [RCS] via the RCV [CVCS] to regulate the boron concentration of reactor coolant | BNX |
| 30 | RGL [RPICS] | Rod Position Indication and Rod Control System | Indicates the position of the control rod in the core, and monitors the failure signal of the control rod and its related equipment as well as indication of these states. The rod control system is used to control of reactor power and coolant temperature | BSA/B/C Safeguard Building |
| 31 | RIS [SIS] | Safety Injection System | Provides emergency borated water injection to compensate for loss of water inventory (e.g. LOCAs) | BSA/BSB/ BSC, BRX |
| 32 | RPR [RPS] | Reactor Protection System | Collects the protection parameters for the detection of Design Basis Condition (DBC) events and once the protection parameters reach or exceed specified set-points, then it triggers the required protection functions automatically or manually (e.g. reactor trip, turbine trip, safety injection etc.) | Safeguard Building (BSA/B/C) |

T-B-1 Summary of the Function and Principal Locations of Plant Systems Considered to be Within the GDA Scope

| No | System Code | System Description | Function(s) | Key Locations(s) |
|---|---|---|---|---|
| 33 | RRI [CCWS] | Component Cooling Water System | Removes heat (via heat exchangers) from equipment located in the NI. Closed loop system which delivers heat to SEC [ESWS] | BMX, BSA/BSB/ BSC |
| 34 | SEC [ESWS] | Essential Service Water System | Delivers heat load transferred from RRI to the ultimate heat sink (3 trains) | BPA/BPB |
| 35 | TEG [GWTS] | Gaseous Waste Treatment System | Processes radioactive gaseous wastes released from the reactor coolant and controls their release to the environment | BNX |
| 36 | TEP [CSTS] | Coolant Storage and Treatment System | Receives, stores and treats reusable primary coolant during normal operation | BNX |
| 37 | VDA [ASDS] | Atmospheric Steam Dump System | Removes residual heat by discharging steam from steam generator into atmosphere | BSA/BSB/ BSC, BRX |
| 38 | VVP [MSS] | Main Steam System | Transfers steam from the SGs to a common main steam header in BMX | BRX, BSA/BSB/ BSC/ BMX |
| Instrumentation and Control Systems | | | | |
| 39 | KDA [SA I&C] | Severe Accident I&C System | I&C for severe plant conditions | BSA/BSB |

T-B-1 Summary of the Function and Principal Locations of Plant Systems Considered to be Within the GDA Scope

| No | System Code | System Description | Function(s) | Key Locations(s) |
|---|---|---|---|---|
| 40 | KDS [DAS] | Diverse Actuation System | Diverse means of protection to PS | BSA |
| 41 | KIC [PICS] | Plant Computer Information & Control System | Provides shift personnel with sufficient control means, information and operating guides for the monitoring and control of the plant | BSC (MCR), RSS |
| 42 | KPR [RSS] | Remote Shutdown Station System | The KPR [RSSS] enables the operators to perform adequate operation, to make the reactor reach a safe shutdown status when the MCR is unavailable due to an independent external or internal hazard | MCR, RSS, TSC |
| 43 | KRT [PRMS] | Plant Radiation Monitoring System | Indicates that the radiological conditions in the plant are within the bounds of the designed conditions | BSA/BSB |
| 44 | KSC [MCRS] | Main Control Room System | Control and monitoring equipment needed by the shift team to perform the essential functions of the power plant from MCR | BSC (MCR) |

T-B-1 Summary of the Function and Principal Locations of Plant Systems Considered to be Within the GDA Scope

| No | System Code | System Description | Function(s) | Key Locations(s) |
|---|---|---|---|---|
| 45 | RIC [ICIS] | In-core Instrumentation System | Measures neutron flux, temperature and RPV level for normal and post-accident monitoring | BRX, BSA/BSB/ BSC |
| 46 | RPN [NIS] | Nuclear Instrumentation System | Measures and monitors reactor nuclear power constantly from reactor start-up to full power operation | BSA/BSB/ BSC, BRX |
| Supporting Systems | | | | |
| 47 | DCL [MCRACS] | Main Control Room Air Conditioning System | Maintains ambient conditions (temperature, humidity and cleanliness) within the acceptable range for personnel and equipment in MCR | BSC |
| 48 | DVD [DBVS] | Diesel Building Ventilation System | Provides ventilation for three trains of EDGs and two trains of SBO diesels | BDA/BDB/ BDC, BDU/BDV |
| 49 | DVW [ABUAVS] | Access Building Uncontrolled Area Ventilation System | Maintains ambient conditions (temperature, humidity and cleanliness) within the acceptable range for personnel and equipment in BPX | BPX |

T-B-1 Summary of the Function and Principal Locations of Plant Systems Considered to be Within the GDA Scope

| No | System Code | System Description | Function(s) | Key Locations(s) |
|---|---|---|---|---|
| 50 | DWK [FBVS] | Fuel Building Ventilation System | Maintains ambient conditions (temperature, humidity and cleanliness) within the acceptable range for personnel and equipment in BFX | BFX |
| 51 | DWL [SBCAVS] | Safeguard Building Controlled Area Ventilation System | Maintains ambient conditions (temperature, humidity and cleanliness) within the acceptable range for personnel and equipment in BSA/BSB/BSC | BSA/BSB/ BSC, BFX |
| 52 | DWN [NABVS] | Nuclear Auxiliary Building Ventilation System | Maintains ambient conditions (temperature, humidity and cleanliness) within the acceptable range for personnel and equipment in BNX | BNX |
| 53 | DWQ [WTBVS] | Radioactive Waste Treatment Building Ventilation System | Maintains ambient conditions (temperature, humidity and cleanliness) within the acceptable range for personnel and equipment in BWX | BWX |
| 54 | DWW [ABCAVS] | Access Building Controlled Area Ventilation System | Maintains ambient conditions (temperature, humidity and cleanliness) within the acceptable range for personnel and equipment in BPX | BPX |

T-B-1 Summary of the Function and Principal Locations of Plant Systems Considered to be Within the GDA Scope

| No | System Code | System Description | Function(s) | Key Locations(s) |
|---|---|---|---|---|
| 55 | EBA [CSBVS] | Containment Sweeping and Ventilation System | Controls containment pressure and provides fresh air during shutdown modes. | BFX, BRX |
| 56 | LAA/B/C/D [NI-DCPS(220V-2h)] | 220V DC Power Supply in NI(2h) | NI 2h DC and AC Uninterruptible Power Supply (UPS) systems | BSA/BSB/BSC |
| 57 | LAP/Q [NI-DCPS(220V-12h)] | 220V DC Power Supply in NI(12h) | NI 12h DC and AC UPS system | BSA/BSB |
| 58 | LGA/B/C/D/E/F/G/H [CI-NPDS(10kV)] | CI 10kV Normal Power Distribution System | Provides AC supplies to loads required to support power generation | CI |
| 59 | LGM/N/O/P/Q [NI-NPDS(10kV)] | NI 10kV Normal Power Distribution System | Provides power to NI | NI |
| 60 | LHA/B/C [EPDS(NI-10kV)] | NI 10kV AC Emergency Power Distribution System | Emergency power distribution to NI | NI |
| 61 | LHM/N [SBOPDS(NI-10kV)] | NI 10kV SBO Power Distribution System | SBO power distribution to NI | NI |
| 62 | LHP/Q/R [EPPS(NI-10kV)] | NI 10kV AC Emergency Power Supply System | Emergency power distribution to NI | NI |
| 63 | LHU/V [SBOPPS(NI-10kV] | NI 10kV SBO Power Supply System | SBO power distribution to NI | NI |
| 64 | LLA/B/C/D/E/F/G/H/I/J/K/M/N/S/T/U/V [EPDS(NI-AC 380V)] | NI 380V Emergency Power Distribution System | Emergency power distribution to NI | NI |
| 65 | LOA/B/C/D/E/F [I&C PDS(NI-380V)] | NI 380V I&C Power Distribution System | NI Power distribution | NI |

T-B-1 Summary of the Function and Principal Locations of Plant Systems Considered to be Within the GDA Scope

| No | System Code | System Description | Function(s) | Key Locations(s) |
|---|---|---|---|---|
| 66 | LVA/B/C [NI-AC-UPS-380-2h] | NI-380V AC Uninterruptible Power Supply System 2h | NI 2h DC and AC UPS systems | BSA/BSB/ BSC |
| 67 | LVD [NI-UPS(220V-2h)] | NI 220V Uninterruptible Power System | NI 2h DC and AC UPS System | BSC |
| 68 | LVP/Q [NI-AC-UPS-380-12h] | NI 380V AC Uninterruptible Power Supply System 12h | NI 12h DC and AC UPS system | BSA/BSB |
| 69 | PMC [FHSS] | Fuel Handling and Storage System | All equipment used for fuel handling and storage | BRX, BFX |
| 70 | REN [NSS] | Nuclear Sampling System | Provides monitoring for determining the physical and chemical characteristics via on-line devices and obtaining samples from the primary systems, secondary systems and other auxiliary systems | BNX |
| 71 | RPE [NIVDS] | Nuclear Island Vent and Drain System | Collects recyclable coolant effluents, unrecyclable liquid wastes and gaseous wastes from the nuclear island | BRX, BSA/BSB/ BSC, BFX, BNX, BPX |
| 72 | SRE [SRS] | Sewage Recovery System | Collects liquid radioactive waste from plant outside NI | BWX, BBH |
| 73 | SEL [LWDS(CI)] | Conventional Island Liquid Waste Discharge System | Monitors and discharges potentially contaminated liquid effluent to the environment. | CI |

T-B-1 Summary of the Function and Principal Locations of Plant Systems Considered to be Within the GDA Scope

| No | System Code | System Description | Function(s) | Key Locations(s) |
|---|---|---|---|---|
| 74 | TER [NI-LWDS] | NI Liquid Waste Discharge System | Monitor and discharges treated liquid radioactive effluent to the environment | BWX |
| 75 | TES [SWTS] | Solid Waste Treatment System | Manages solid radioactive wastes generated during operation (e.g. filters, resins) | BWX |
| 76 | TEU [LWTS] | Liquid Waste Treatment System | Receives, stores and treats the radioactive liquid waste generated in normal operation | BWX |

# Annex C Potential Initiating Events of Malicious Origin and Associated Potential Targets

*Annex C has been redacted as it contains classified information.*

# Annex D Locations of UK HPR1000 Candidate Vital Areas

*Annex D has been redacted as it contains classified information.*

# Annex E Threat Interpretation

# 1. Physical Security Threat Determination

## 1.1 Introduction

This annex assesses the physical security threat to the generic design of the UK HPR1000 using the UK's DBT to the security of civil nuclear sites within the UK. The planning assumptions for the UK's DBT for security are presented within NIMCA (Reference [10]).

The defining factor for including a planning assumption in the threat interpretation is based on whether the assumption can cause a URC through the theft or sabotage of NM/ORM or SSCs that maintain the nuclear inventory in a safe condition. Assumptions that may support the creation of a URC have been accepted, and those assumptions that do not were rejected. This means that the assumptions that are accepted will contribute to the creation of an IEMO or compromise SSCs as part of a SEC.

## 1.2 Redacted Information

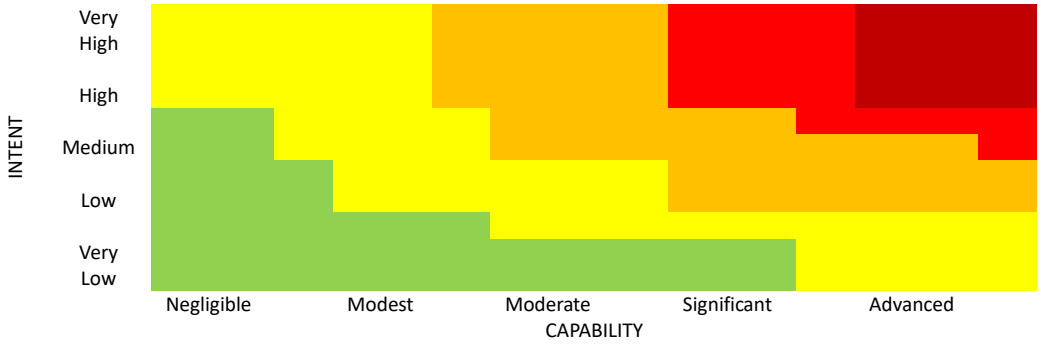
*The physical planning assumptions using the malicious capabilities within the NIMCA document are classified and so the remainder of Section 1 of Annex A has been redacted.*

# 2. Cyber Security Threat Determination

## 2.1 Threat Ranking

### 2.2.1 Likelihood Matrix

The following matrix was developed within Reference [8] to assess the intent and capability of threat sources and threat actors. For continuity, this approach has been adopted and modified within this determination.




### 2.2.2 Definition of Intent

The following definitions of threat source intent are used within this determination:

- Very High – The action is a very high priority for the threat source and activities are ongoing or almost certain to occur in the immediate future. The threat source will expend several man years of effort supported by considerable funds.
- High – The action is a high priority for the threat source and the activities occur often or are very likely to occur. The threat source will expend a few years of effort and moderate funds.
- Medium – The action is a medium priority for the threat source and the activity occurs on a periodic or regular basis. The threat source will expend up to one man year of effort and modest funds.
- Low – the action is a low priority for the threat source and the activity will only occur on an infrequent basis or in specific circumstances (e.g. periods of heightened tension). The threat source will expend up-to six months of effort and limited funds.
- Very Low – the action is not a priority for the threat source, and activities are not planned. Activities are limited to inadvertent actions and targets of opportunity. The threat source will expend limited effort (days or weeks) and very limited funds.

### 2.2.3 Definition of Capability

The following definitions of threat source capability are used within this determination:

- Advanced – The threat source has significant technical resources to acquire significant data on the target system, reverse engineer systems and develop bespoke cyber-attacks. In addition, the threat source can sustain prolonged effort, an insider and has physical intrusion capabilities. Typically, capability at this level is limited to Hostile State Actors (HSA).
- Significant – The threat source has advanced technical resources and is able to acquire data on the target system, has limited capability to reverse engineer

systems and has the capability to generate bespoke cyber-attacks when required. In addition, the threat source is assumed to be able to support reasonable durations of operations, an insider and physical intrusion capabilities, although these may be limited to a regional basis. Typically, this is limited to less capable HSA.

- Moderate – The threat source has moderate technical resources, and whilst having a reasonable repertory of open source techniques, bespoke techniques are limited. Data gathering on targets is also limited. The threat source can undertake activities with a typical duration of a year, can support an insider and may have a limited physical intrusion capability.
- Modest – The threat source has very limited capability for data gathering and / or developing bespoke attacks. The threat actor will be limited in tactics and will use open source attack methods / exploits. The threat source cannot mount sustained operations, and is unlikely to have access to an insider or any physical intrusion capability.
- Negligible – The threat source has no access to intelligence beyond public information and only has the capability to successfully deploy a limited set of open source cyber-attacks. The threat source is limited to attempts to intrude on poorly defended internet connected systems, but with a limited success. The threat actor cannot maintain sustained operations, and will not have an additional insider or any physical intrusion capability. This also applies to those threat sources with greater capabilities who would not deliberately perform these actions.

## 2.2 Threat Sources

The following threat sources are considered within this threat determination (References [8], [9] and [10]):

- Hostile State Actor.
- Terrorists (International or Domestic).
- Hacktivists (to include Anti-Nuclear, Environmental & Local Interest Groups).
- Cyber Criminals (Organised Crime and Petty Criminals).
- Investigative Journalists.
- Disgruntled Employees.
- Commercial Competitors.
- Academia and Research.

### 2.2.1 Threat Summary

T-E2.2-1 overleaf, presents a summary of the intent and capability of the threat sources with regards to both espionage (theft of SNI and other information) and sabotage. It should be noted that there is often a range of capability and intent for each threat actor category depending upon individual threat source and this determination presents the worst case scenario. For example, Hostile State Actor intent and capability vary between nations.

T-E2.2-1 – Worst Case Threat Source Intent and Capability

*T-E2.2-1 has been redacted as it contains classified information.*

## 2.3 Threat Actors

The following section identifies potential threat actors both within the civil nuclear facility, within the associated off-site supply chain or external to the site. It also identifies their capabilities and typical access constraints. It is considered that the threat actor will assume the intent of their associated threat source and that their innate capability may be augmented by the threat source (potentially up to the capability level of the threat source itself – for capable threat actors).

### 2.3.1 Threat Actor Types

Individual threat actors have been designated as one of the following broad categories:

Privileged User (PU): Such as person would legitimately be granted physical and logical access to operational and safety critical infrastructure. The level of access would include maintenance access. In addition, due to the nature of their job, they would have significant technical knowledge of the system, as well as access to the associated supporting technical and safety documentation.

Normal User (NU): Such a person would have legitimate physical and logical access to the system to a level required to perform their duties (e.g. access to Human Man Interfaces and system features required to operate the system). Their duties would include access to operational and safety critical equipment. In addition, by the nature of their job, they would have an understanding of how the system operated, as well as access to the associated supporting operational documentation. They would however, not be provided with maintenance access or maintainer level knowledge of system operations.

Person Within Range (PWR): Such a person would legitimately be granted access to site and possibly into areas containing operational or safety critical equipment. However, they would not be given physical access to equipment or logical access to such systems. As such they would not have access to operational, technical or safety documentation associated with operational or safety critical equipment. Such personnel would typically have a minimal understanding of the operation / maintenance or significance of equipment.

Supply Chain (SISC): It should be noted that persons within the supply chain also have access to the systems or their associated design documents during system development and could be considered Privileged Users (typically system designers / developers) or Persons Within Range (e.g. handlers / delivery staff).

External Actors: Any additional threat actor group has been identified – External Actor which covers any unauthorised person external to site who attempts to gain access to the site either directly or via existing logical connections to the outside world.

### 2.3.2 Identification of Threat Actors

A number of individual threat actors have been identified and are listed below.

- Maintenance Engineer / Repairer / Tester
- System Administrator / Plant Supervisor
- Plant Operator / System User

- Librarian
- Site Visitor
- Site Security Personnel
- Non-Technical Personnel
- System Developer / Designer
- Support Engineer
- Handler
- Emanation
- External Unauthorised User

### 2.3.3 Threat Actor Competencies

The threat actors and threat sources have also been grouped in terms of their technical competence / skill levels in accordance with the annexes to ONR Security Principles Reference [1] in T-E2.3-1 below.

T-E2.3-1 – Threat Actor / Source Competency / Skill Level

*T-E2.3-1 has been redacted as it contains classified information.*

# Annex F Concept of Operations Framework

**T-F-1 CONOP Framework**

| CONOP Section | SyAP Principle | Section Owner | Synopsis |
|---|---|---|---|
| 1. Objectives of the CONOP | | RP | The objective of the CONOP will be stated. This will be to effectively manage all the security risks relevant to the processing, handling and storage of NM/ORM at the UK HPR1000 site to ensure that the latter is not compromised. Full implementation of the CONOP will ensure that the security regime remains effective at all times. |
| 2. Description of the Site and Site Operations | SyDP 6.5<br>SyDP 6.6 | RP | This section will present a description of the UK HPR1000 site, including an outline of the reactor plant and fuel handling and storage facilities and processes. It will present a map showing size of the site, the site layout and its geographical location.<br><br>It will identify the assets (NM/ORM, VAs, CBSIS and CBSy) to be protected, and a map will be included showing the site boundary, locations of the NM/ORM, security zones and security barriers. Reference will be made to the next section for more details on the NM/ORM.<br><br>Details of the site operations will be provided, included the average numbers of personnel and contractors who will be employed on the site.<br><br>The site will be considered in relation to adjacent or enclave nuclear premises, and nuclear construction sites. The impact that the UK HPR1000 site will have on surrounding sites will be identified and addressed in relevant sections of the CONOP. |
| 3. Categorisation for Theft | SyDP 6.1<br>SyDP 6.4 | RP | This section will present a list of the type, category and location of all the NM and ORM at the UK HPR1000 site. It will present the expected changes to the NM/ORM inventory and location during site operations. This presentation of the NM/ORM holdings will be supported by plot plans showing their locations.<br><br>The categorisation for theft will also consider the vulnerability assessments that have been undertaken and identify where they have been addressed in the CONOP. |

**T-F-1 CONOP Framework**

| CONOP Section | SyAP Principle | Section Owner | Synopsis |
|---|---|---|---|
| | | | Protective measures to prevent the theft of SNI will be included in Section 15. |
| 4. Categorisation for Sabotage | SyDP 6.2<br>SyDP 6.4 | RP | This section will present all of the VAs by categorisation and classification, CBSIS and CBSy by location at the UK HPR1000 site. This presentation will be supported by plot plans showing their locations.<br><br>The categorisation for sabotage will also consider the vulnerability assessments that have been undertaken and identify where they have been addressed in the CONOP. |
| 5. Threat and Regulatory Requirements for Security | SyAPs | RP | This section will describe the threat to the site that the CONOP will mitigate and the Regulatory security requirements that need to be satisfied. This will include, but not be limited to:<br>a) Reference to the UK's Design Basis Threat.<br>b) Security outcomes, responses and postures. |
| 6. The Management of Security | SyDP 1.1<br>SyDP 1.2<br>SyDP 1.3<br>SyDP 1.4<br>SyDP 1.5<br>SyDP 2.1 | SL | This section will present the security organisation and roles. More specifically, it will include a description of the roles, responsibilities and terms of reference for:<br>a) Corporate Level (Board) Person Accountable.<br>b) Facility Management Roles and Responsibilities (including Command and Control Responsibilities during Emergency Situations).<br>c) Security Manager.<br>d) Deputy Security Manager.<br>e) Civil Nuclear Constabulary (CNC) Commander.<br>f) Numbers and primary responsibilities of CNC personnel.<br>g) Security (Shift) Team Leader.<br>h) Security Department Staff/Guards.<br>i) Response Arrangements for both internal and external agencies.<br><br>Additionally, this section will describe how the following will be implemented and maintained during site operations: |

**T-F-1 CONOP Framework**

| CONOP Section | SyAP Principle | Section Owner | Synopsis |
|---|---|---|---|
| | | | a) Security Culture.<br>b) Audit of security procedures (e.g. personnel vetting, security training).<br>c) Security Performance Assessments. |
| 7. Access Control Measures to Limited Access Area | KSyPP 3<br>KSyPP 4<br>KSyPP 5<br>SyDP 6.3 | RP | This section will describe the access control measures in place at the UK HPR1000 site. |
| 8. Access Control Procedures to Limited Access Areas | KSyPP 3<br>KSyPP 4<br>KSyPP 5<br>SyDP 6.3 | RP | This section will describe the access control procedures in place at the UK HPR1000 site. |
| 9. Protected Area Perimeter Security Arrangements | KSyPP 3<br>KSyPP 4<br>KSyPP 5<br>SyDP 6.3 | RP | This section will describe the access security measures and procedures in place for the High Security Area at the UK HPR1000 site. |
| 10. Inner Area (IA)/ Higher Risk Vital Area Security Arrangements | KSyPP 3<br>KSyPP 4<br>KSyPP 5<br>SyDP 6.3 | RP | This section will describe the security arrangements (measures and procedures) for limiting access to sensitive areas (i.e. areas containing NM/ORM, VAs, CBSIS and CBSy) within the IA and/or Higher Risk Vital Area to authorised personnel only. |
| 11. Other Building Security Arrangements | KSyPP 3<br>KSyPP 4<br>KSyPP 5<br>SyDP 6.3 | RP | This section will describe the security arrangements (measures and procedures) for limiting access to sensitive areas out with the High Security Area to authorised personnel only. |
| 12. Command, Control, Communication | SyDP 5.1<br>SyDP 10.3 | SL | This section will describe the C3I infrastructure at the UK HPR1000 site. |

**T-F-1 CONOP Framework**

| CONOP Section | SyAP Principle | Section Owner | Synopsis |
|---|---|---|---|
| and Intelligence (C3I) | | | |
| 13. Main Control Room and Emergency Control Room Security Arrangements | SyDP 7.1<br>SyDP 7.2<br>SyDP 10.1<br>SyDP 10.3 | RP | This section will describe the security arrangements for the Main Control Room (MCR) and the Emergency Control Centre (ECC) at the UK HPR1000 site. This will include a description of the access security measures and procedures. |
| 14. Cyber Security | SyDP 7.1<br>SyDP 7.5 | RP | This section will describe the cyber security arrangements at the UK HPR1000 site and will include:<br>a) Detection of: viruses; malware; unauthorised changes.<br>b) Network monitoring.<br>c) Test rig for software updates/patches.<br>d) Resilient system architecture.<br>e) Procedures to maintain:<br>i. Security awareness.<br>ii. Control over 3rd party remote diagnostics.<br>iii. Isolation from internet.<br>iv. Integrity of network (i.e. control over emails and portable media).<br>v. Access controls.<br>vi. Integrity of updates/modifications. |
| 15. Information Security | SyDP 7.2<br>SyDP 7.3<br>SyDP 7.4 | SL | This section will describe the arrangements for the security of information at the UK HPR1000 site. This will cover all information on the site including Sensitive Nuclear Information, Protectively Marked Information and Personal Information. |
| 16. IT Security | SyDP 7.1 | SL | This section will describe the security arrangements for the use of IT equipment (e.g. desktop computers, laptops, printers, USB drives, phones etc) on the UK HPR1000 site. This will encompass IT equipment permanently used within the site as well as equipment brought onto the site. |
| 17. Personnel | SyDP 8.1 | SL | This section will describe the personnel security arrangements at the UK HPR1000 site. This will |

**T-F-1 CONOP Framework**

| CONOP Section | SyAP Principle | Section Owner | Synopsis |
|---|---|---|---|
| Security/ Trustworthiness | SyDP 8.2<br>SyDP 8.3 | | include:<br>a) Clearance level requirements to access NM/ORM, sensitive or protectively marked information.<br>b) Key and Combination Controls.<br>c) Pass Issue Equipment Control and Supervision.<br>d) Management Supervision and Role in Aftercare.<br>e) Maintenance of a good security culture throughout the site.<br>f) The reliability and trustworthiness of individuals who either have unescorted or escorted access to, or detailed knowledge of, NM/ORM, VAs, CBSIS and CBSy. |
| 18. Transport of NM | SyDP 6.7 | SL | This section will describe the security arrangements for the transport of NM within the UK HPR1000 site. |
| 19. Control of Security Incidents | SyDP 9.2<br>SyDP 10.1<br>SyDP 10.2<br>SyDP 10.3 | SL | This section will describe the procedures in place for the control of security incidents on the UK HPR1000 site. |
| 20. Security Forces | SyDP 9.1<br>SyDP 9.3 | SL | This section will describe the roles and responsibilities of the Guard Force and the integration with the CNC at the UK HPR1000 site. |
| 21. Maintenance of Security | SyDP 5.1<br>SyDP 5.2<br>SyDP 5.3 | SL | This section will describe the auditing and testing of the maintenance, testing and repair of the security systems for the UK HPR1000 site. |
| 22. Nuclear Supply Chain Management | SyDP 4.1<br>SyDP 4.2<br>SyDP 4.3<br>SyDP 4.4 | SL | This section will describe the roles and capabilities expected of both the customer and the supplier. This will include the security measures and processes expected at the supplier's site.<br><br>Requirements for the Intelligent Customer will be stated. These will include how the Intelligent Customer will deliver oversight of the suppliers of items or services that may impact on security, and |

**T-F-1 CONOP Framework**

| CONOP Section | SyAP Principle | Section Owner | Synopsis |
|---|---|---|---|
| | | | how such items will be commissioned. |
| 23. Education and Training | SyDP 3.1<br>SyDP 3.2<br>SyDP 3.3<br>SyDP 3.4 | SL | This section will describe the education and training requirement for the UK HPR1000 site. This will include:<br>a) Standards of education and training for professional security personnel.<br>b) Standards of security training for site employees and contractors.<br>c) Integration of training between the Guard Force and CNC, and the latter with site management and safety personnel.<br>d) Frequency of training for professional security personnel.<br>e) Frequency of security training for site employees and contractors.<br>f) Training on security culture. |
| 24. List of Security Instructions and Procedures | | SL | This section lists all the UK HPR1000 Site Security Instructions and Security Procedures. |