A Holtec International Company

Holtec Britain Ltd	HI-2240261
Sponsoring Company	**Document Reference**
0	30 September 2024
Revision No.	**Issue Date**
Report	Non-proprietary
Record Type	**Proprietary Classification**
ISO 9001	No
Quality Class	**Export Control Applicability**

Record Title:

Preliminary Security Report

Proprietary Classification

This record does not contain commercial or business sensitive information.

Export Control Status

Export Control restrictions do not apply to this record.

Revision Log

Revision	Description of Changes
0	First Issue to Regulators

Table of Contents

List of Figures

List of Tables

Commercially Confidential Information

Portions of this document that is enclosed with curly brackets “{…}” is Holtec Commercially Confidential Information.

1.0 INTRODUCTION

1.1 Overview

Holtec International (Holtec) is planning to deploy its 300 MWe Small Modular Reactor (SMR-300) in the United Kingdom (UK). To support this, Holtec (via its UK Division, Holtec Britain) is submitting its SMR-300 design for Steps 1 and 2 of the Generic Design Assessment (GDA) process by the UK nuclear regulators, namely the Office for Nuclear Regulation (ONR), the Environment Agency (EA) and Natural Resources Wales (NRW).

The focus of the overall assessment in the two-step GDA is towards the fundamental adequacy of the design and the safety, security, safeguards, and environmental cases. This includes determination of the suitability of the methodologies, approaches, codes, standards, and philosophies which form the building blocks for the design and the generic security case.

Hence, to complete Steps 1 and 2 of the GDA, Holtec is required to submit security documentation for assessment by the regulators during both steps of the GDA. This document, the Preliminary Security Report (PSyR), is the security submission to ONR in support of Step 1 of the GDA.

1.2 Aim and Objectives of the GDA Step 1 Preliminary Safety Report

The overall aim of this PSyR is to provide ONR with the confidence that it will be able to undertake a 'meaningful assessment' of the security topic during Step 2 and thereby contribute positively towards the ONR Step 1 public statement that the SMR-300 can proceed to Step 2 of the GDA[1].

This aim is achieved through the following objectives:

- Demonstrate an understanding of the UK nuclear regulatory security framework and how the design will be compliant;
- Provide the basis for the development of the nuclear security arrangements, including the security philosophy and principles;
- Provide SMR-300 design familiarisation information for the ONR security assessors to understand the context for the nuclear security case;
- Present an outline of the nuclear security case[2] and the main security claims, showing how these claims integrate with the overall high level SMR-300 safety, security and environmental claims;
- Outline the evolution of this PSyR to Generic Security Report (GSR) Revision 1 in GDA Step 2 and how GSR Rev 1 will integrate with the safety and environmental cases.

1.3 Scope and Exclusions

The scope of the SMR-300 GDA Step 2 nuclear security submission is focused on the methodologies, approaches, codes, standards, and philosophies which together will form the

[1] A meaningful assessment is defined by ONR as having received sufficient information in the GSR to allow assessment within the agreed GDA scope for the topic.
[2] This term is used in this document to mean the entirety of documentation submitted to the ONR to justify the nuclear security of the SMR-300 plant.

building blocks for the development of the site security case and site security arrangements/security plan.

In addition to presenting the methodologies, the Step 2 scope includes an illustration of the implementation of the methodologies using an area within the plant and a system which will road-test the different aspects of the Vital Area identification and cyber security risk assessment methodologies respectively to build confidence that they are suitable and sufficient for use in subsequent project stages. This will assist ONR in their assessment that the methodologies proposed are adequate and, if implemented by a site licensee, would lead to an SMR-300 design compliant with legislative and regulatory requirements (as defined in Section 3.0).

The following are excluded from the GSR scope:

- Facilities, buildings, operations or systems not identified in [1];
- Sensitive Nuclear Information (SNI) located on a future SMR-300 site;
- Assessment of malicious aircraft impact;
- The provision of equipment for safeguards purposes (note that this is addressed by [2]).

The depth of assessment will depend on the design maturity available in GDA Step 2. Hence for some systems, such as Computer Based Security Systems (CBSy), high level consideration only is anticipated.

1.4 Structure of the Preliminary Security Report

This PSyR delivers the above objectives as follows:

Table 1: Structure of PSyR

Section	Presents:
3.0	Holtec's understanding of the international and UK legislative and regulatory framework for nuclear security
4.0	The philosophy and principles which will be applied to develop the SMR-300 nuclear security case
5.0	Scope of the GDA and plant information for the SMR-300
6.0	Outline of the SMR-300 security case
7.0	Delivery of security
8.0	The evolution of this document to the GDA Step 2 Generic Security Report

2.0 ABBREVIATIONS

2.1 Project Abbreviations

Term	Definition
AR	Annular Reservoir
ADS	Automatic Depressurisation System
ALARP	As Low as Reasonably Practicable
CAE	Claims, Argument, Evidence
CBSIS	Computer Based Systems Important to Safety
CBSy	Computer Based Security Systems
CBV	Containment Ventilation System
CES	Containment Enclosure Structure
CGC	Combustible Gas Control System
CNS	Civil Nuclear Security
CONOP	Concept of Operations
CPPNM	Convention on the Physical Protection of Nuclear Material
CPS	Cyber Protection System
CS	Containment Structure
CSH	Overhead Heavy Load Handling System
CSRA	Cyber Security Risk Assessment
DAC	Design Acceptance Confirmation
DBA	Design Basis Accident
DBT	Design Basis Threat
DESNZ	Department for Energy Security & Net Zero
DFSS	Dry Fuel Spent Storage
DRP	Design Reference Point
EA	Environment Agency
ESF	Engineered Safety Features
FSyP	Fundamental Security Principles
GB GSE	Great Britain Generic Site Envelope
GDA	Generic Design Assessment
GSR	Generic Security Report
HMG	His Majesty's Government
I&C	Instrumentation and Control
IAEA	International Atomic Energy Agency
ICSANT	International Convention for the Suppression of Acts of Nuclear Terrorism
IRP	Inherent Risk Profile
ISS	Integrated Security Solution
KSyPP	Key Security Plan Principles
LLH	Light Load Handling System
LOCA	Loss of Coolant Accident
MDSL	Master Document Submission List
MWe	Mega Watt Electric
NCSC	National Cyber Security Centre

Term	Definition
NFSV	New Fuel Storage Vault
NISR	Nuclear Industries Security Regulations
NM	Nuclear Material
NORMS	National Objectives, Requirements and Model Standards
NPSA	National Protective Security Authority
NRW	Natural Resources Wales
NSS	Nuclear Security Series
NSSP	Nuclear Site Security Plan
ONR	Office for Nuclear Regulation
ORM	Other Radioactive Material
O-S	Official-Sensitive
PCC	Passive Core Cooling System
PCM	Passive Core Makeup Water System
PDH	Primary Decay Heat Removal System
PPS	Physical Protection System
PSgR	Preliminary Safeguards Report
PSyR	Preliminary Security Report
PWR	Pressurised Water Reactor
RAB	Reactor Auxiliary Building
RCA	Radiologically Controlled Area
RCCA	Rod Cluster Control Assembly
RGP	Relevant Good Practice
RI	Regulatory Issue
RO	Regulatory Observation
RP	Requesting Party
RQ	Regulatory Query
RR SMR	Rolls-Royce Small Modular Reactor
S	Secret
SA	Security Architecture
SAPs	Safety Assessment Principles
SbD	Secure by Design
SDH	Secondary Decay Heat Removal System
SFP	Spent Fuel Pool
SI	Security Infrastructure
SIRO	Senior Information Risk Owner
SME	Subject Matter Expert
SMR	Small Modular Reactor
SMR-300	300 MWe Small Modular Reactor
SNI	Sensitive Nuclear Information
SPF	Security Policy Framework
SSC	Structure, System and Component
SSEC	Safety, Security and Environmental Case
SyAP	Security Assessment Principles

Term	Definition
SyC	Security Claim
SyDP	Security Delivery Principles
TAG	Technical Assessment Guide
TIG	Technical Inspection Guide
TRD	Technical Requirements Document
URC	Unacceptable Radiological Consequence
UK	United Kingdom of Great Britain and Northern Ireland
USNRC	United States Nuclear Regulatory Commission
VDR	Vendor Design Review
VAI&C	Vital Area Identification and Categorisation
WENRA	Western European Nuclear Regulators Association

3.0 LEGISLATIVE AND REGULATORY FRAMEWORK

3.1 Introduction

This section summarises international and UK regulation and guidance which inform Holtec's understanding of the requirements and expectations for nuclear security for the SMR-300 in the UK and hence are reflected by the philosophies, principles and approaches outlined in this PSyR.

3.2 International Regulation and Guidance

The UK is signatory to two international conventions which are relevant to the legislative framework for the protection of Nuclear Material (NM), Other Radioactive Material (ORM) and SNI:

a) As a member state of the International Atomic Energy Agency (IAEA) and a signatory to the Convention on the Physical Protection of Nuclear Material (CPPNM) [3] and its amendment [4]), the UK is obliged to establish and maintain a framework which provides for the application of physical protection requirements and include a system of evaluation, permissioning and compliance inspection, together with a means of enforcement, including effective sanctions;
b) The United Nations International Convention for the Suppression of Acts of Nuclear Terrorism (ICSANT) [5]. In particular, Article 8 requires signatories to make every effort to adopt appropriate measures to ensure the protection of radioactive material, considering recommendations and functions of IAEA.

Furthermore, both conventions refer to the IAEA and the relevant guidance which it provides in these areas.

IAEA's objective for a State's nuclear security regime is to protect persons, property, society, and the environment from harmful consequences of a nuclear security event. To achieve this objective, a State should establish, implement, maintain, and sustain an effective and appropriate nuclear security regime to prevent, detect and respond to such nuclear security events.

Within IAEA, the Nuclear Security Series (NSS) provides international consensus guidance on all aspects of nuclear security to support States as they work to fulfil their responsibility for nuclear security. The series comprises four sets of publications:

- Nuclear Security Fundamentals [6], which establishes the fundamental objective and essential elements of a State's national nuclear security regime;
- Recommendations, which set out measures that States should take to achieve and maintain an effective regime;
- Implementing Guides, which provide guidance on how States can implement the Recommendations;
- Technical Guidance, which provide more detailed guidance on specific methodologies and techniques for implementing security measures.

Of relevance to a security submission during GDA are:

- Nuclear Security Recommendations on the Physical Protection of Nuclear Material and Nuclear Facilities, NSS No 13 (INFCIRC225 Revision 5) [7];

- Identification of Vital Areas at Nuclear Facilities, Technical Guidance Document NSS No. 16 [8];
- IAEA Nuclear Security Series No. 4 Engineering Safety Aspects of the Protection of Nuclear Power Against Sabotage [9].

In addition, the Western European Nuclear Regulators Association (WENRA) has published guidance on the interfaces between nuclear safety and nuclear security [10] which provides recommendations for promoting synergy between safety and security assessments, resolving conflicts and the importance of the application of a security by design philosophy early in the design of new plants.

3.3 UK Regulation

In the UK, these international obligations are currently achieved primarily through two pieces of legislation, namely:

- The Energy Act (2004) defines the provisions which establish ONR as a statutory body, describes its purposes (one of which is nuclear security) and establishes its powers;
- The Nuclear Industries Security Regulations (NISR) 2003.

The regulations are enforced by the Civil Nuclear Security (CNS) section of the ONR.

NISR 2003 (as amended) ([11]) places significant obligations on the operators of civil licensed nuclear sites relating to physical security measures for facilities, nuclear material and the security of SNI, ensuring that the prime responsibility for the implementation of arrangements for protection of NM, ORM, and associated facilities and SNI rests with the dutyholder.

During the GDA process, the principal applicability of NISR 2003 is in relation to the protection of SNI which may be generated or handled by the Requesting Party (RP). An outline strategy for compliance with these requirements of NISR during GDA is presented in Appendix A.

NISR 2003 also requires that all civil nuclear operators in the UK must produce and implement robust Nuclear Site Security Plans (NSSPs). While not directly applicable to the GDA process, the GDA submissions, including this PSyR and the subsequent GSR Version 1 must ensure that the generic methodologies and arrangements developed must be suitable for future development into an NSSP by a future operator in accordance with NISR 2003, or to otherwise not foreclose options which a future operator may choose to implement.

3.4 ONR Guidance

The regulation of civil nuclear security in the UK began its transition towards non-prescriptive civil nuclear security regulations over a decade ago. Prior to 2012, CNS enforced NISR 2003 in a prescriptive manner as defined in the extant NISR 2003 Technical Requirements Document (TRD).

In 2012, in line with the UK government policy on regulation at the time, CNS started transitioning the regulation of civil nuclear security towards a goal setting, outcome focused approach analogous to that established for safety regulation via the ONR's Safety Assessment Principles (SAPs) [12]. CNS published a National Objectives, Requirements and Model Standards (NORMS) document which set out best practice. The dutyholder was required follow these standards or propose alternative justified measures (for example where the standards could not be achieved), that met the same national objectives.

In 2017, CNS fully transitioned the regulation of civil nuclear security to a non-prescriptive regime. In support of this, the first Security Assessment Principles (SyAPs) document ([13]) was issued. The SyAPs cover physical security, personnel security, cyber security and information assurance, and transport security.

SyAPs present ten fundamental security principles (FSyPs) that define general security outcomes that the dutyholder must deliver. These FSyPs are either strategic enablers or are focused on the delivery of the security operations. Each of the FSyPs is supported by one or more Security Delivery Principles (SyDPs). The SyDPs support the dutyholder in the delivery of the FSyPs by presenting Relevant Good Practice (RGP).

The SyAPs document also defines a set of seven Key Security Plan Principles (KSyPPs), which present the basis for an effective security plan and are applied across the FSyPs and SyDPs covered in a security plan.

Following five years of regulation experience using the 2017 SyAPs, which included their application to operational nuclear facilities as well as their use in both new build licensing and the GDA process, the SyAPs document was reviewed and re-issued in 2022 to reflect the learning gained during this period. The 2022 SyAPs are currently being used in the GDAs for the first set of SMRs undergoing this pre-licensing process.

Hence, SyAPs provide ONR with a baseline against which to make regulatory judgements on the adequacy of security arrangements. In general, SyAPs reflect ONR's expectations for security submissions within a goal-setting and outcome-based framework and are benchmarked against international good practice and IAEA guidance. The SyAPs are themselves supported by Technical Assessment Guides (TAGs), and other guidance, to further assist decision making within the nuclear security regulatory assessment process.

Within the scope of this GDA, the following TAGs are particularly relevant:

- Categorisation for Theft (CNS-TAST-GD-6.1) [19];
- Categorisation for Sabotage (CNS-TAST-GD-6.2) [20];
- Physical Protection System Design (CNS-TAST-GD-6.3) [21];
- Protection Of Nuclear Technology and Operations (CNS-TAST-GD-7.3) [22];
- Secure by Design (CNS-TAST-GD-11.4.1) [23];
- The Threat (CNS-TAST-GD-11.4.2) [24];
- Guidance on the Security Assessment of Generic New Nuclear Reactor Designs (NS-TAST-GD-11.1) [25].

ONR uses the SyAPs and TAGs to guide their regulatory judgements when undertaking assessments of security submissions. These will form the basis of ONR's judgement of the adequacy of the security case for the SMR-300.

Whereas not all of the SyAPs are directly applicable during the GDA process, the expectation is that the security arrangements detailed in the GSR will be suitable to meet regulatory expectations so to be of value to a future operator.

To facilitate the delivery of proportional security, the SyAPs define a graded set of Physical Protection System (PPS) and Cyber Protection System (CPS) outcome and response effects together with indicative security postures within a series of protectively marked Annexes. The

duty holder is required to meet the protection outcome and response effects but is given flexibility on how the outcomes and response effects are met provided that the security solution is justified. The Annexes also provide further details on the level of Unacceptable Radiological Consequence (URC) to be considered in the security case as well as criteria for categorisation for theft and Vital Areas.

3.4.1 Specific GDA Security Guidance

The principal source of guidance for a GDA security assessment is the Guidance on the Security Assessment of Generic New Nuclear Reactor Designs [25]. This TAG contains guidance to inform ONR inspectors in exercising their regulatory judgment during assessment activities related to the adequacy of generic designs for new nuclear reactors.

The GDA Guidance to Requesting Parties [26] provides more general detail on ONR's expectations for the GDA process. This outlines a three-step approach for GDA, with the ultimate expectation (at the end of Step 3) being for RPs to '*produce a Generic Security Report (GSR) that describes a conceptual security regime that will be developed further by a prospective Licensee for a Site Licence Grant application'* which should '*describe the security features of the proposed design. It should document the categorisation from both theft and sabotage to determine the protective security outcomes and applicable security postures to be applied'*.

However, the GDA for the SMR-300 will conclude at Step 2. [26] states that '*For a GDA that completes at Step 2, ONR will provide a GDA Statement*' and it explains that '*there are a number of potential outputs that can be provided upon completing a GDA. The output provided will depend on the GDA scope agreed, the meaningfulness of the assessment undertaken, the adequacy of the safety and security cases submitted and the significance of any residual safety or security concerns that remain to be resolved*'.

Thus, Holtec's expectations are that the ONR GDA Step 2 statement would be consistent with the statements made at the end of Step 2 in previous GDAs, defined in [26] as ONR will produce and publish a GDA Statement summarising:

a) *Details of the status of the design and associated generic safety and security cases, including the MDSL and DRP;*
b) *The assessment of the submissions provided by the RP during Step 2;*
c) *Details of the readiness review conducted to determine if the RP can continue to Step 3;*
d) *Any open regulatory questions (RQs, ROs, and RIs);*
e) *Any areas of regulatory concern to be taken forward in later Steps;*
f) *Any significant issues that may prevent ONR from issuing a DAC, might prevent ONR permissioning construction of a Nuclear Power Plant based upon that design or which might be in conflict with Government policy.*

In the case of a two-step GDA, cases c) and e) above are interpreted to refer to site licensing rather than 'Step 2' and 'later Steps' respectively and f) is not applicable.

The sampling process in [26] highlights that *'…ONR focuses on, in broad terms…the overall design and safety and security claims, as well as the methodologies, approaches, codes, standards and philosophies during Step 2*', noting that this has been used to derive the scope presented in sub-section 1.3. [27] provides RGP for the security documents provided during a

GDA. This is reflected by the proposed document structure for GDA Steps 1 and 2, namely the development of a Preliminary Security Report (this document) in Step 1 which provides the outline of a GSR structure (and required supporting methodologies and analyses) to be developed during Step 2.

3.4.2 UK Relevant Good Practice

An expectation for the GDA is that the security submissions will draw upon RGP. In addition to examples of RGP outlined by ONR's TAGs and Technical Inspection Guides (TIGs), other RGP may be identified through:

- Security submissions from current and previous GDAs, specifically for the Rolls-Royce Small Modular Reactor (RR SMR) and UK HPR1000 which were regulated under SyAPs;
- ONR summary reports and feedback on the above;
- Information and guidance from industry bodies and associations such as National Protective Security Authority (NPSA) and National Cyber Security Centre (NCSC).

The assessment methodologies developed by Holtec during GDA Step 2 will consider RGP identified from UK and international sources in areas such as Vital Area identification, cyber security risk assessment and secure by design.

3.4.3 International Relevant Good Practice

In addition to international guidance identified earlier, RGP may be identified from security submissions to international regulators including, for example to the CNSC's Vendor Design Review (VDR) process.

In developing the SMR-300 security case for the UK, Holtec will seek to draw upon, and learn lessons from, the development of security arrangements for the SMR-300 in international markets, including feedback from the US NRC licensing process.

4.0 SECURITY PHILOSOPHY AND PRINCIPLES

4.1 Introduction

This section outlines, at a high level, the philosophy and principles which will be applied to develop the SMR-300 nuclear security case. These have been influenced by consideration of KSyPPs 1, 3 and 4 [13]; Secure by design, the graded approach and Defence in Depth respectively.

The security philosophy and principles will underpin the evolution of the nuclear security case will evolve from this PSyR, to the Step 2 GSR and, ultimately, into the NSSP.

4.2 Security Philosophy

A risk-informed, proportionate, and holistic approach will be followed to protect nuclear material and SNI[3] at an SMR-300 site through life which:

- Delivers security by design by seeking to integrate measures into the developing design rather than adding them later;
- Security-informs the design and layout of the plant from as early as possible in the design development (and modification) process;
- Integrates the security case with (in particular) the safety and safeguards cases;
- Incorporates a Secure by Design (SbD) hierarchy of risk controls (KSyPP 1);
- Is consequence-based to enable proportional (graded) protective measures to deliver the security objectives (KSyPP 3);
- Recognises that whilst design and engineering is a key enabler to the management of security risk and delivery of the most effective means of risk control (see
- Figure 2), a robust security management system and culture are required during all stages of the project lifecycle to minimise the risk as shown in Figure 1 below.

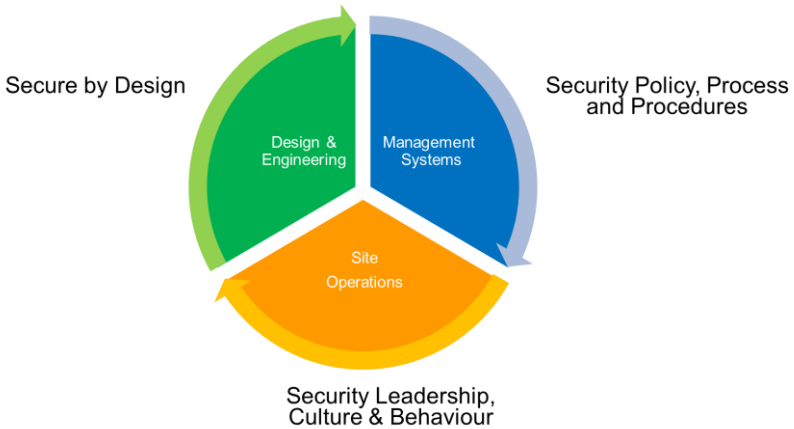

Figure 1: Security Risk Control Enablers

- (REDACTED)

[3] UK nuclear security legislation and regulation requires the protection of SNI at the site. However, this is outside the scope of the GDA as the presence and extent of SNI at a site are site-specific.

- Recognises that protection is provided via a holistic and integrated blend of physical, cyber and procedural measures which build on design and safety case robustness measures to provide defence in depth (KSyPP 4), rather than considering them as individual measures;
- Ensures that nuclear security arrangements will need to integrate seamlessly with the wider security arrangements at the site;
- Recognises that nuclear security is an enabler for safe and secure SMR-300 operations and not an inhibitor.

4.2.1 Secure by Design Principle

The SMR-300 SbD is influenced by KSyPP 1 and aims to deliver an inherently secure design by seeking to eliminate, or reduce, security vulnerabilities during the design process rather than address these later in the development lifecycle by retrospectively adding protective or mitigative security measures.

(REDACTED)

This hierarchy will be applied when considering key design decisions or assessing modifications to the plant during the GDA programme and will help to guide the design firstly towards ‘designing out’ security vulnerabilities or otherwise providing passive protection (e.g., plant robustness) in preference to adding active security features such as access control or a response force.

The secure by design principle can be illustrated by Figure 2 below:

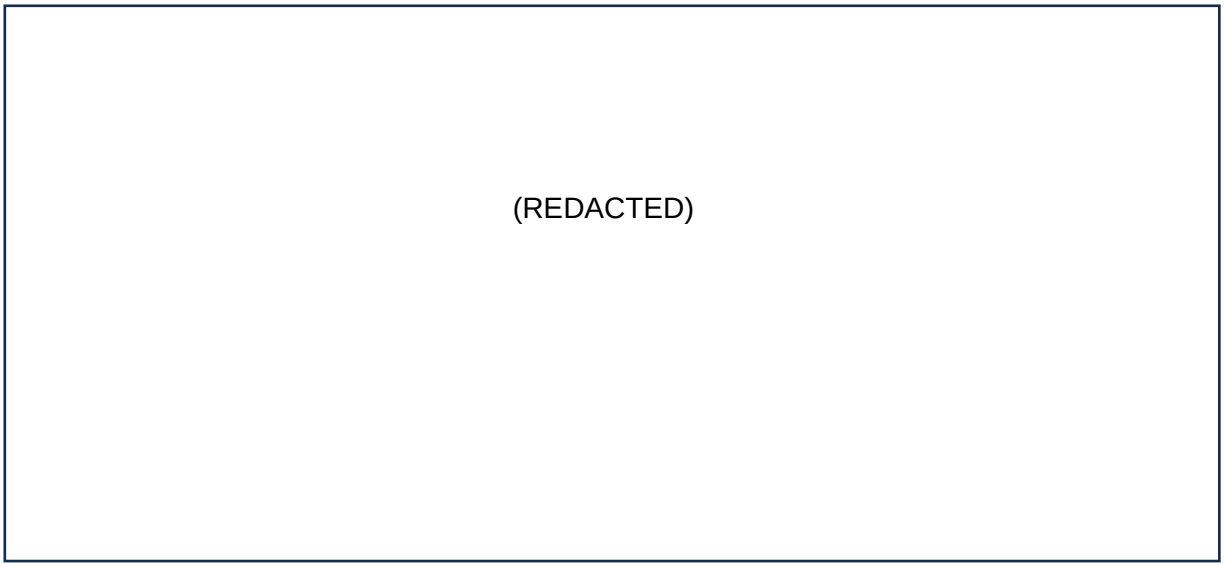

Figure 2: (REDACTED)

This hierarchy recognises that the most effective means of reducing security vulnerability and achieving an inherently secure design are through elimination of vulnerabilities, substitution of processes or through passive engineering. Furthermore, making appropriate design decisions provides for a long-term reduction in the capital and operational costs of providing physical

security at the facility because of the reduction in the need for, and reliance on, protective security systems.

Examples of how security-informed design can eliminate or reduce security vulnerabilities include:

(REDACTED)

Examples of more general SbyD activities are associated with ensuring that the design can accommodate, and be influenced by, security requirements, such as:

(REDACTED)

Hence, the application of the secure by design principle ensures that the SMR-300 design is informed by the security requirements that need to be considered in design activities and decision making, which is supported by the derivation of outline security design principles (see sub-section 6.5). Design activities in this context refer to a range of activities during the project lifecycle including:

(REDACTED)

4.2.2 Defence in Depth Principle

The defence in depth principle (KSyPP 4) ensures that the integrated security solution is composed of multiple layers and approaches which together ensure that an adversary would need to overcome several independent barriers to achieve its objective.

In many cases, the security assessment benefits from defence in depth inherent in the safety design of the plant; for example,

(REDACTED)

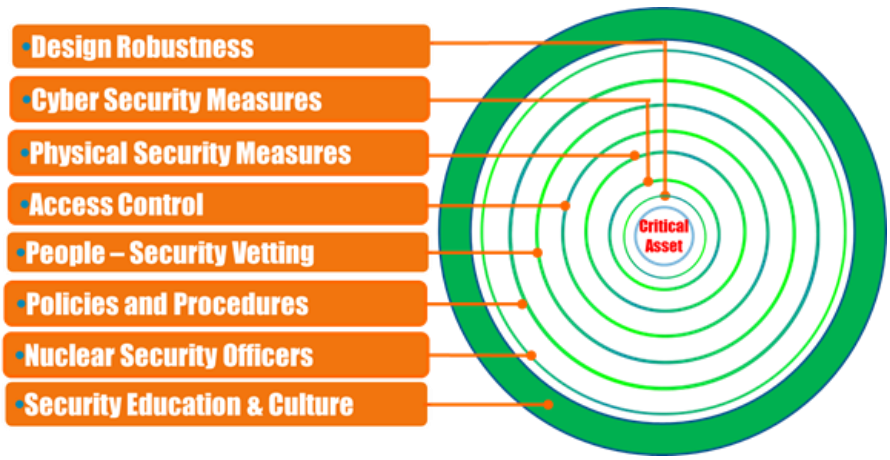

Figure 3: Defence in Depth

4.2.3 Integrated Security Solution

As highlighted in Figure 4, an integrated security solution incorporates layers of measures associated with:

(REDACTED)

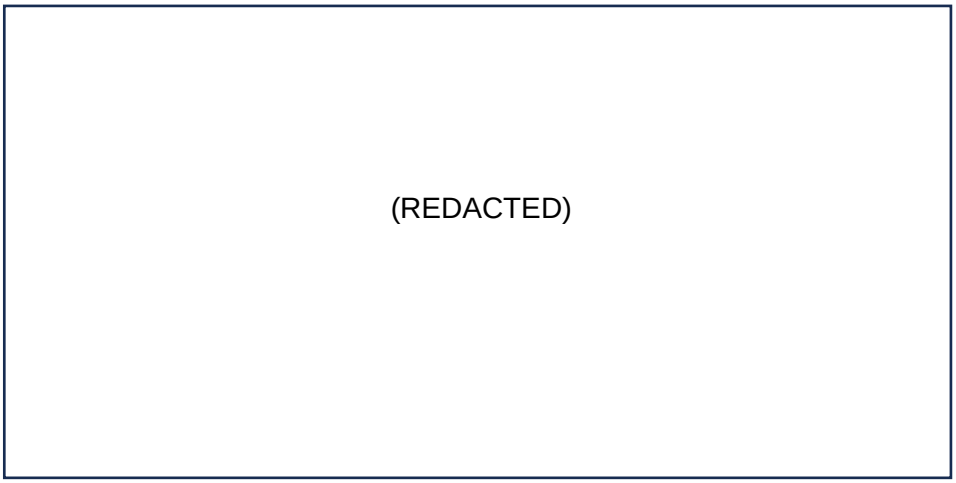

Figure 4: (REDACTED)

5.0 SCOPE OF GDA AND PLANT INFORMATION

5.1 Scope

The scope of the GDA is outlined in [1]. In line with this, the Safety, Security and Environmental Case (SSEC) will be developed for a twin-unit reactor design to be constructed, operated, and decommissioned on a generic site that bounds all prospective sites considered within the SMR-300 Great Britain Generic Site Envelope (GB GSE).

Hence, the GSR will consider only those buildings, operations and systems which are included within [1].

5.2 Plant Information

5.2.1 Overview

(REDACTED)

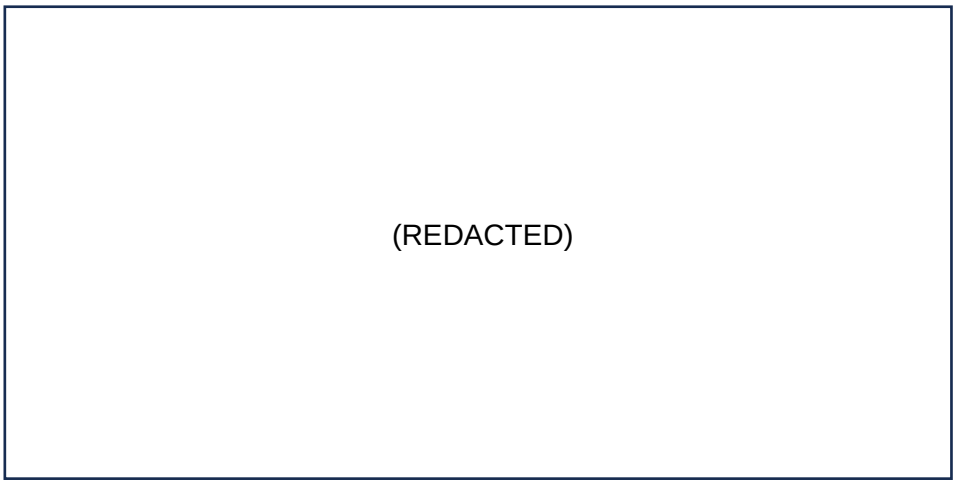

Figure 5: (REDACTED)

(REDACTED)

5.2.2 Containment Structure

(REDACTED)

5.2.3 Containment Enclosure Structure

(REDACTED)

5.2.4 Reactor Auxiliary Building

(REDACTED)

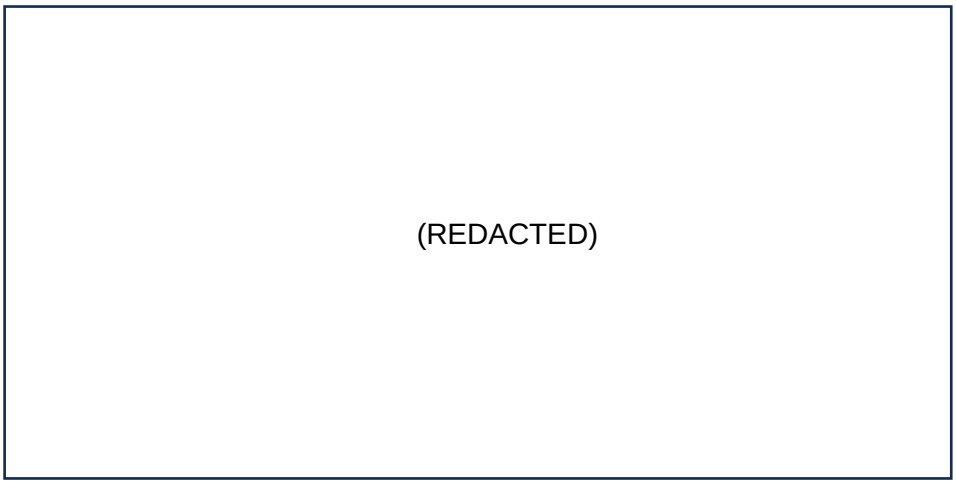

Figure 6: (REDACTED)

5.2.5 Secure by Design Considerations

The design process to date has included consideration of the SbyD principle and the risk hierarchy of controls (see sub-section 4.2.1 and Figure 2) as outlined below.

(REDACTED)

6.0 NUCLEAR SECURITY CASE

6.1 Introduction

In line with the above philosophy and principles, nuclear security for the SMR-300 plant will be delivered via the following series of activities which, taken together, provide a structured, clear, and logical approach to the development of the conceptual security arrangements for the SMR-300.

The key steps of this approach are:

(REDACTED)

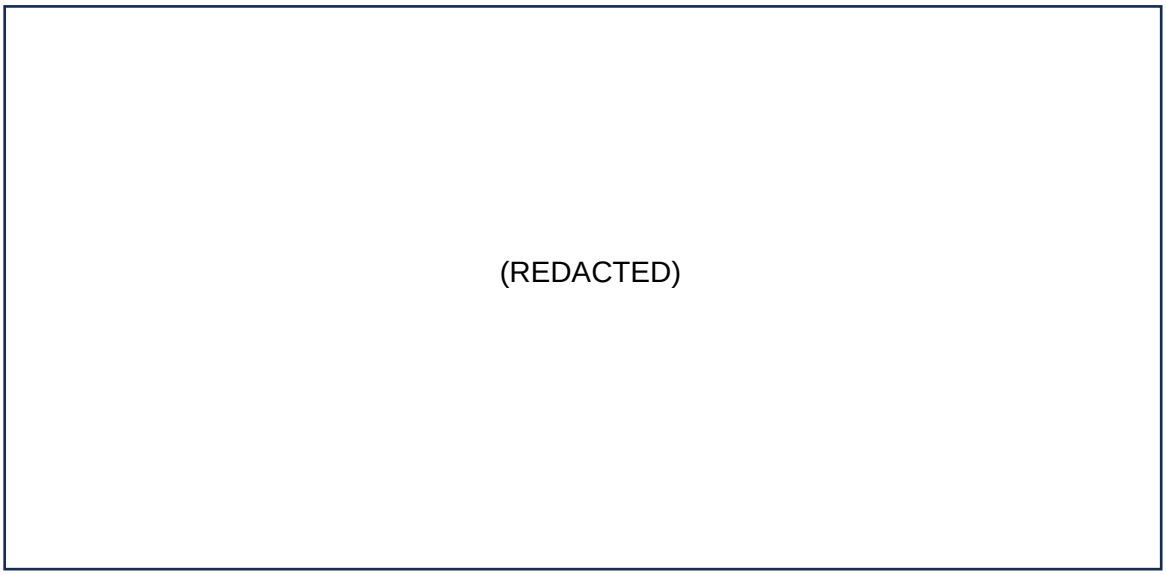

Figure 7: (REDACTED)

6.2 Security Claims

The fundamental objective of the SMR-300 security case is to demonstrate that security risks are managed to protect workers and the public from a radiological event arising from the theft or sabotage of nuclear or radioactive material or through the compromise of SNI.

This aim is supported by seven outline high-level Security Claims (SyCs) which will be delivered by the SMR-300 security case as it evolves from this PSyR into the GSR and, ultimately, to the NSSP (see Figure 8 below). These claims reflect the structured delivery approach outlined in Figure 7.

[4] (REDACTED)
[5] **{**REDACTED**}**
[6] (REDACTED)

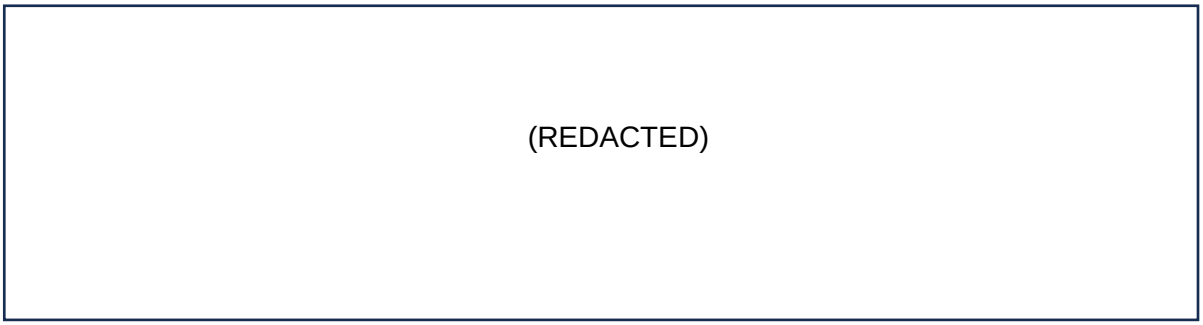

Figure 8: (REDACTED)

6.3 Security Sub-Claims

The seven SyCs identified in Figure 8 will be decomposed into sub-claims, arguments and evidence (as possible and proportionate with the Reference Design maturity) during GDA Step 2. Examples of this initial break-down are provided below which will provide a framework for subsidiary arguments to be developed:

(REDACTED)

6.4 Integration with the Safety, Environmental and Safeguards Case

(REDACTED)

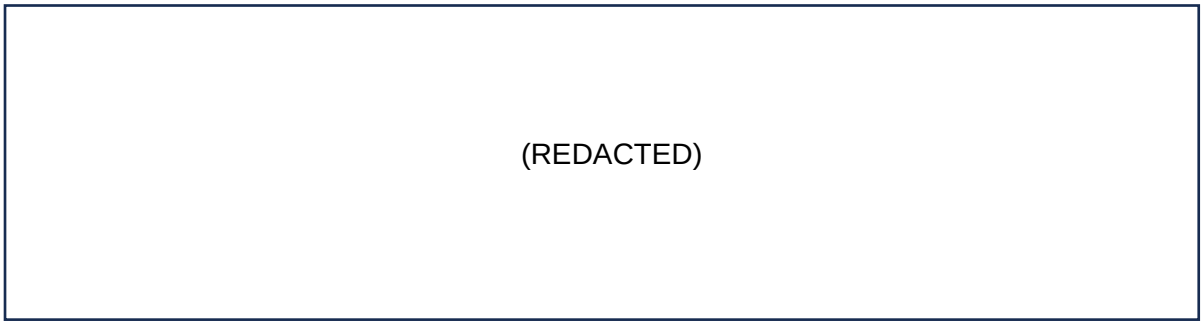

Figure 9: (REDACTED)

6.5 Security Design Principles

An initial suite of security-informed design principles will be developed early in Step 2 to support the implementation of SyC 5 (Security-influenced Design) during the design process, in line with [29], including for:

- Aid to design decision making;
- (REDACTED);

- (REDACTED);
- Providing a 'golden thread' for demonstration of design optimisation.

(REDACTED)

The key elements of the SMR-300 secure by design process are illustrated in Figure 10 and an overview is given below.

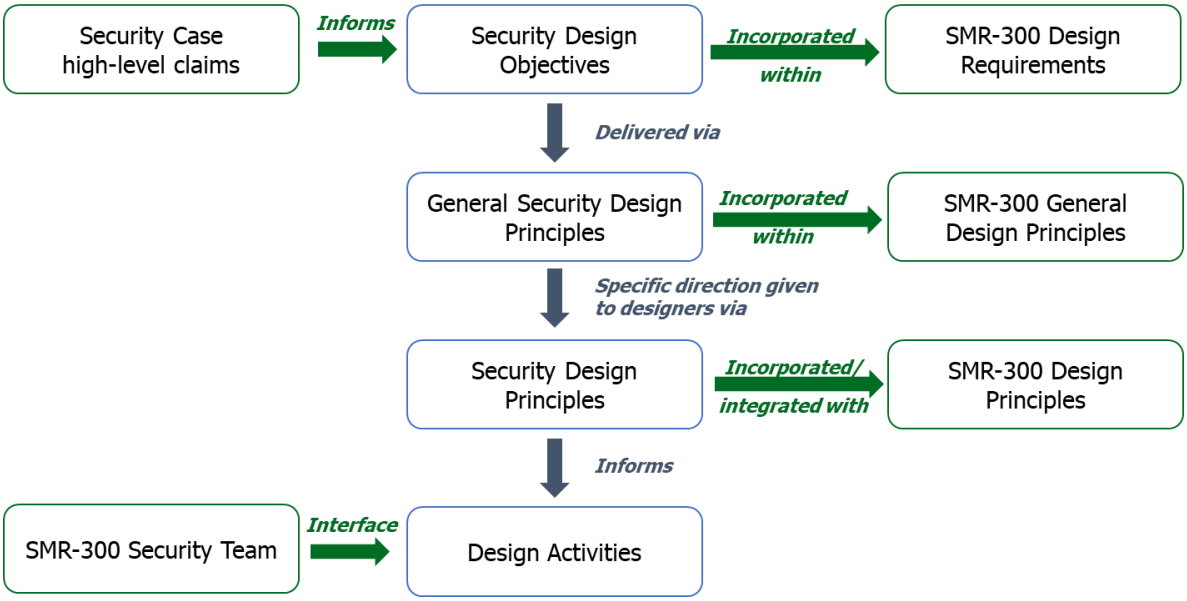

Figure 10: SMR-300 Integration of Secure by Design with Design Process

6.5.1 Design Activities

The SyDPs will inform the SMR-300 designers of the security requirements that need to be considered in design activities. Design activities in this context refer to a range of activities during the project lifecycle including:

- Design of the SMR-300 site and building layouts;
- Design of plant SSCs;
- ALARP and Optioneering studies;
- Design Reviews;
- Design Modification;
- Design of plant upgrades.

The SMR-300 Security Team is involved in design activities, by providing advice on individual design activities, resolving conflicts between safeguards requirements and other disciplines, or participating in ALARP/Optioneering studies or design review committees.

7.0 DELIVERY OF SECURITY

7.1 Introduction

(REDACTED)

7.2 Identification of Assets and Areas for Protection

7.2.1 Introduction

(REDACTED)

7.2.2 Sabotage

(REDACTED)

7.2.3 Theft

(REDACTED)

7.3 Threat Interpretation

7.3.1 Introduction

For application within security assessments, the threat is determined by the UK government and stems from an (REDACTED)

7.3.2 Approach

(REDACTED)

a) (REDACTED);
b) (REDACTED);
c) (REDACTED);
d) The design of protective measures;
e) The design of the overall security solution;
f) The evaluation of site security operations.

The methodology will include a review/update process to ensure that the threat interpretation remains up to date with a changing threat landscape through the course of the project.

7.3.3 Application of Threat in GDA Step 2 Security Assessments

(REDACTED)

7.3.4 Application of Threat Post GDA Step 2

(REDACTED)

7.4 Protection of Assets and Vital Areas

7.4.1 Introduction

(REDACTED)

7.4.2 Cyber Security Risk Assessment

(REDACTED)

7.4.3 Conceptual Security Arrangements

The outputs of the VAI&C and CSRA will form an input into the development of the required security architecture and infrastructure for the generic security arrangements to protect the SMR-300. Together this provides the ISS.

These arrangements provide proportionate and integrated security that, together:

- Deliver a proportionate defence in depth security regime;
- (REDACTED)
- (REDACTED)

Security Architecture (SA) describes the network architecture that is required to support the security arrangements. (REDACTED)

In addition, high-level expectations for the required Management Systems and Site Operations will be identified for further consideration during the site licensing process.

(REDACTED)

7.5 Security Operations

(REDACTED)

8.0 EVOLUTION INTO THE GDA STEP 2 GENERIC SECURITY REPORT

8.1 Introduction

This PSyR will develop into the GSR at GDA Step 2 which will represent the (developing) Security Case for the generic SMR-300 and will be structured in such a way as to facilitate further development into a site-specific Security Case and, ultimately, into a NSSP.

8.2 Objectives of the Generic Security Report

The objectives of GSR, and its supporting documents, are to:

- Provide suitable and sufficient plant design and operation information (within the agreed GDA scope of assessment) to enable understanding of the GSR by a technical reader[7];
- Demonstrate how the evolving design is compliant with the UK nuclear security regulatory framework;
- Outline the security claims, arguments and evidence showing how these claims integrate with the overall high-level SMR-300 safety, security, safeguards and environmental claims;
- Demonstrate how the security philosophy and principles are being adopted;
- (REDACTED)
- Demonstrate how the nuclear security case and security arrangements are being developed;
- Outline the evolution to subsequent issues of the GSR or to site licensing and the NSSP.

8.3 Structure of the Generic Security Report

The intention is for the GSR to form a head document at ‘claims’ level and to be structured in a similar format to this PSyR for continuity purposes. Two versions of this head document will be presented in Step 2 to enable the GSR to be subject to public comments. The public version may require redaction of any commercially sensitive or security-related information.

The head document GSR will be supported by several claims-level ‘Tier 2’ documents which will provide Topic Reports supporting the GSR, including for:

(REDACTED)

Each Topic Report will include a methodology for the topic which will be developed in line with UK requirements and RGP. This will be informed by, and report on, a pilot study application of the methodology on an agreed limited-scope aspect of the SMR-300 design (which itself is reported in detail at Tier 3 where appropriate). Tier 2 will include an outline (REDACTED) document which will provide an (REDACTED)

[7] This may be by a separate section/appendix or by reference to supporting documentation.

Where required, for example for trials of methodologies, a more detailed evidence-level Tier 3 document may be developed to support the Tier 2 documents.

This tiered approach is highlighted in Figure 11 which shows the structure of the GSR Rev 1 document suite consistent with the Claims, Argument, Evidence (CAE) approach around which this is developed, which is outlined further in Table 2.

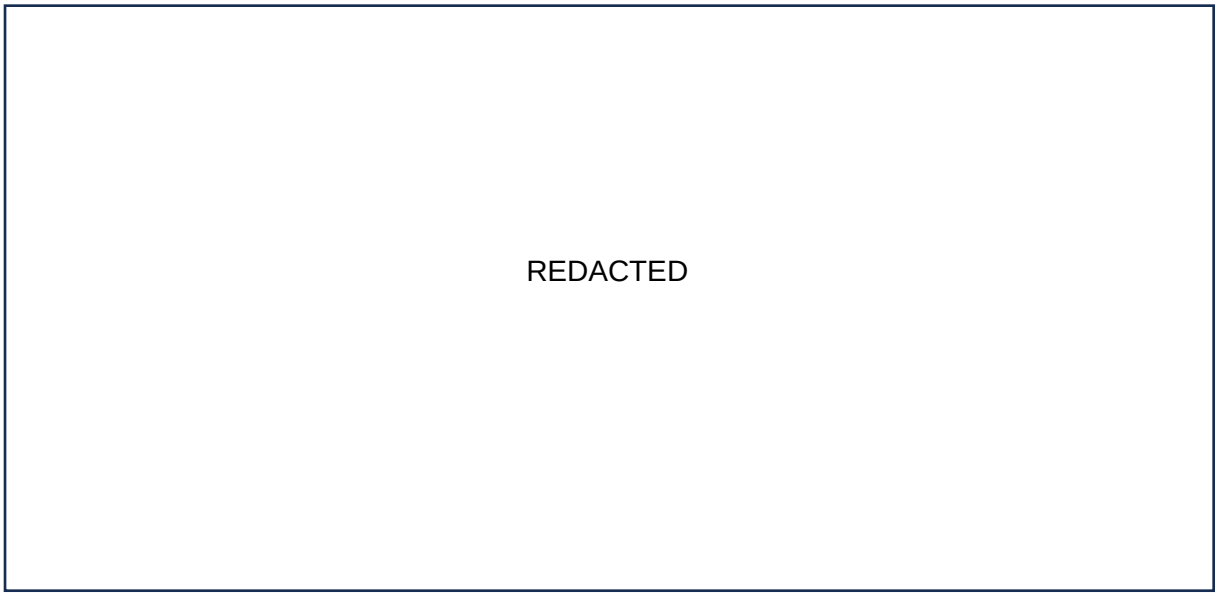

Figure 11: (REDACTED)

Table 2: SMR-300 GSR Rev 1 Document Suite Tiered Approach

Tier	Presents:	Notes
1	The **claims** and **high-level arguments** with appropriate signposts to the detailed arguments and evidence presented in the supporting Tier 2 and 3 documents.	The GSR Head document will be an evolution of this PSyR.
2	The **detailed arguments** supporting the claims. In particular the methodologies to be used for the various security analysis and assessments required to develop the security arrangements.	These will be new reports. It is expected that reports on all the security topics identified in Figure 11 will be included.
3	Illustrative **evidence** commensurate with the level of design development to demonstrate how the methodologies are being development.	These will be new reports. (REDACTED)

Figure 12 presents an example of the three-tier CAE approach for one topic area. In this case, the head document GSR will identify a claim that (REDACTED). At Tier 2, these claims will be expanded into arguments which identify that an appropriate methodology has been developed

and followed and suitable results have been obtained. At Tier 3, appropriate analysis is presented which supports the (REDACTED)

This structure provides an easy to navigate and transparent approach to CAE and ensures that the ‘golden thread’ which runs from (REDACTED)

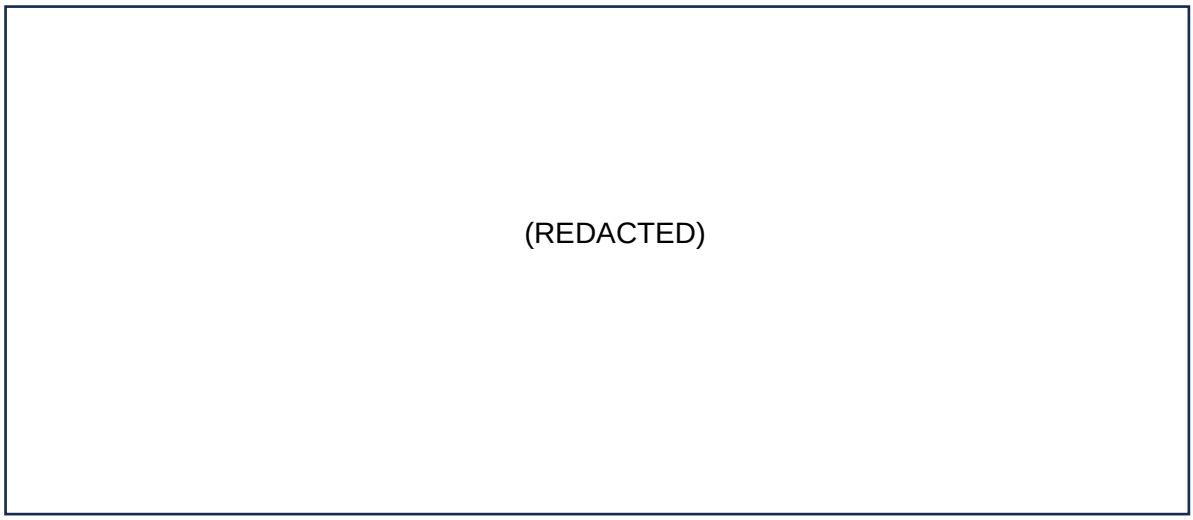

Figure 12: (REDACTED)

8.3.1 Security Classification of GSR Document Suite

(REDACTED)

9.0 REFERENCES

[1] (REDACTED)

[2] (REDACTED)

[3] International Atomic Energy Agency, “Convention on the Physical Protection of Nuclear Material”, October 1979.

[4] International Atomic Energy Agency, “Amendment to the Convention on the Physical Protection of Nuclear Material”, July 2002.

[5] United Nations, “International Convention for the Suppression of Acts of Nuclear Terrorism”, April 2005.

[6] International Atomic Energy Agency, “Nuclear Security Fundamentals, Objective and Essential Elements of a State’s Nuclear Security Regime”, Nuclear Security Series No. 20.

[7] International Atomic Energy Agency, “Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities”, INFCIRC/225/Revision 5.

[8] International Atomic Energy Agency, “Identification of Vital Areas at Nuclear Facilities”, Nuclear Security Series No. 16, 2013.

[9] International Atomic Energy Agency, “Engineering Safety Aspects of the Protection of Nuclear Power Against Sabotage”, IAEA Nuclear Security Series No. 4 (Technical Guidance), 2007.

[10] Western European Nuclear Regulators Association, “Interfaces between Nuclear Safety and Nuclear Security”, April 2019.

[11] HMG Government, “Nuclear Industries Security Regulations (NISR) 2003”, Statutory Instrument 2003, No. 403.

[12] Office for Nuclear Regulation, “Safety Assessment Principles for Nuclear Facilities 2014 Edition”, Revision 1, January 2020.

[13] Office for Nuclear Regulation, “Security Assessment Principles 2022 Edition”, Version 1.

[14] United States Nuclear Regulatory Commission, “Subpart A—General Provisions § 73.1 Purpose and scope”, NRC Regulations Title 10, Code of Federal Regulations.

[15] United States Department of Homeland Security, “Federal Emergency Management Agency (FEMA), Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings”, FEMA 26, December 2003.

[16] ISO/IEC 27005:2022 “Information security, cybersecurity and privacy protection; Guidance on managing information security risks”, Edition 4, October 2022.

[17] International Electrotechnical Commission, “Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels”, IEC 62443, Edition 1.0, 2013.

[18] International Electrotechnical Commission, “Nuclear power plants – Instrumentation, control and electrical power systems – Cybersecurity requirements”, IEC 62645:2019, November 2019.

[19] Office for Nuclear Regulation, “Categorisation for Theft”, CNS-TAST-GD-6.1, Issue 2, June 2023.

[20] Office for Nuclear Regulation, “Categorisation for Sabotage”, CNS-TAST-GD-6.2, Issue 2, March 2023.

[21] Office for Nuclear Regulation, “Physical Protection System Design”, CNS-TAST-GD-6.3, Issue 2, April 2022.

[22] Office for Nuclear Regulation, “Protection of Nuclear Technology and Operations”, CNS-TAST-GD-7.3, Revision 0, March 2017.

[23] Office for Nuclear Regulation, “Secure by Design”, CNS-TAST-GD-11.4.1, Issue 1.1, January 2023.

[24] Office for Nuclear Regulation, “The Threat”, CNS-TAST-GD-11.4.2, Issue 1, April 2022.

[25] Office for Nuclear Regulation, “Guidance on the Security Assessment of Generic New Nuclear Reactor Designs”, CNS-TAST-GD11.1, Issue 1.2, May 2021.

[26] Office for Nuclear Regulation, “Generic Design Assessment Guidance to Requesting Parties”, ONR-GDA-GD-006, Revision 0, October 2019.

[27] Office for Nuclear Regulation, “New Nuclear Power Plants: Generic Design Assessment Technical Guidance”, ONR-GDA-GD-007 Revision 0, May 2019.

[28] (REDACTED)

[29] (REDACTED)

[30] (REDACTED)

[31] Office for Nuclear Regulation, “Information Security”, CNS-TAST-GD-7.2, August 2023.

[32] Office for Nuclear Regulation, “Nuclear Industry Security Regulations 2003-Guidance for Inspectors”, CNSS-SEC-GD-002, Issue 1, Mar 2022.

[33] Office for Nuclear Regulation, “Nuclear Industry Security Regulations, Regulation 22 Dutyholder – Inherent Risk Profile Questionnaire”, Report: 2023/25878.

[34] Government Cabinet Office, “Security Policy Framework”, Dec 2022.

[35] Office for Nuclear Regulation, “Nuclear Industry Security Regulations, Regulation 22 Dutyholder – Evidencing Expectations, System Question Set”, Report: 2023/25877, April 2023.

[36] Office for Nuclear Regulation, “Nuclear Industry Security Regulations, Regulation 22 Dutyholder – Evidencing Expectations, Facility Question Set”, Report: 2023/25876, April 2023.

[37] Office for Nuclear Regulation, “Nuclear Industry Security Regulations, Regulation 22 Dutyholder – Evidencing Expectations, Corporate Question Set”, Report: 2023/25874, April 2023.

[38] HMG Government, “Government Functional Standard”, Report No. GovS 007: Security, Version 2.0, 2021.

[39] Office for Nuclear Regulation, “Security Classification Policy”

[40] Office for Nuclear Regulation Contact Record, “Cyber Security and Information Assurance Regulation 22 meeting with Holtec Britain”, 13 December 2023, Contact Record ID: ONR-CNSS-CR-23-177.

10.0 LIST OF APPENDICES

Appendix A Outline Process for Nuclear Industries Security Regulations (NISR) Compliance NISR

A.1 Introduction

NISR 2003 [11] places legal requirements on organisations to protect nuclear material from sabotage and theft as well as to protect SNI from theft. This means that:

(a) Holtec International, Holtec Britain and their supply chain have the legal requirement (under Part 4, Regulation 22 of NISR 2003) to protect against loss, theft or unauthorised disclosure of, or unauthorised access to SNI whenever it is stored, processed, transmitted or accessed during the SMR-300 GDA and design development.
(b) The SMR-300 licensee will have a legal requirement (under Part 2, Regulations 4 to 12 of NISR 2003) to implement an approved security plan to protect nuclear material at the site from sabotage and theft and to protect against the compromise or loss of SNI within the site.

The following sections provide a description of the process being adopted by Holtec Britain to:

- Comply with the requirements of Regulation 22 of NISR 2003 during the GDA and design development stage (Section 3.0); and
- Facilitate compliance by a future SMR-300 licensee with the requirements of Regulations 4 to 12 of NISR thereafter (Section 4.0).

A.2 SMR-300 GDA and Design Development

This section provides a description of the of the process being adopted by Holtec Britain to comply with the requirements of NISR 2003 during SMR-300 GDA and design development post-GDA.

A.2.1 Protection of SNI

Holtec Britain has developed a pathway to deliver its legal requirement under Regulation 22 of NISR 2003 to protect SNI. The pathway is informed by the ONR SyAPs [13] and supporting ONR guidance [31], [32]. It aims to deliver security management arrangements proportional to the risk based on the quantity and type (Hard copy and/or Digital) of SNI held.

The risk is established using the Inherent Risk Profile (IRP) Questionnaire [33], developed by ONR. The pathway recognises that the IRP level will change for Holtec Britain as the SMR-300 project progresses from GDA Step 1 to Step 2, and thereafter site licensing and operations. A high-level illustration of the pathway showing the change in IRP level and proportional security arrangements is given in Figure 13.

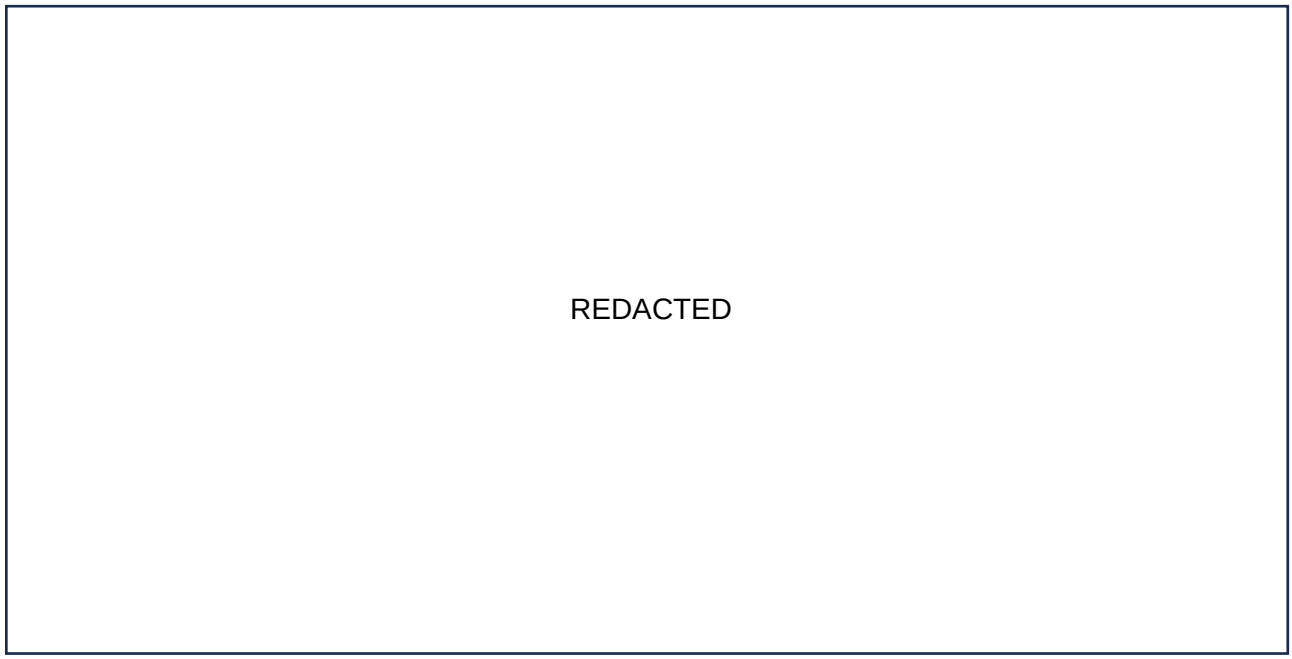

Figure 13: List N Pathway

The key steps comprising the pathway are described below.

A.2.2 Pre-GDA

In preparation to enter the GDA, Holtec Britain undertook a review of its existing security management system relative to the His Majesty's Government (HMG) Security Policy Framework (SPF)[8] [34]. The reviews made use of the ONR Evidencing Expectations [35], [36], [37]to identify gaps relative to the five applicable FSyPs[9] for the different IRP levels:

- FSyP 1 – Leadership and Management for Security;
- FSyP 2 – Security Organisational Culture;
- FSyP 3 – Management of Human Performance;
- FSyP 7 – Cyber security and Information Assurance;
- FSyP 8 – Workforce Trustworthiness.

[8] The HMG Government Functional Standard GovS 007 [32] has replaced the Security Policy Framework. However, the policies which sit within the SPF remain in effect but are now in support of GovS 007.
[9] ONR considers that these 5 FSyAPs provide a framework for compliance with GovS007/SPF.

The review covered the five key elements comprising a security management system, as illustrated in Figure 14[10] .

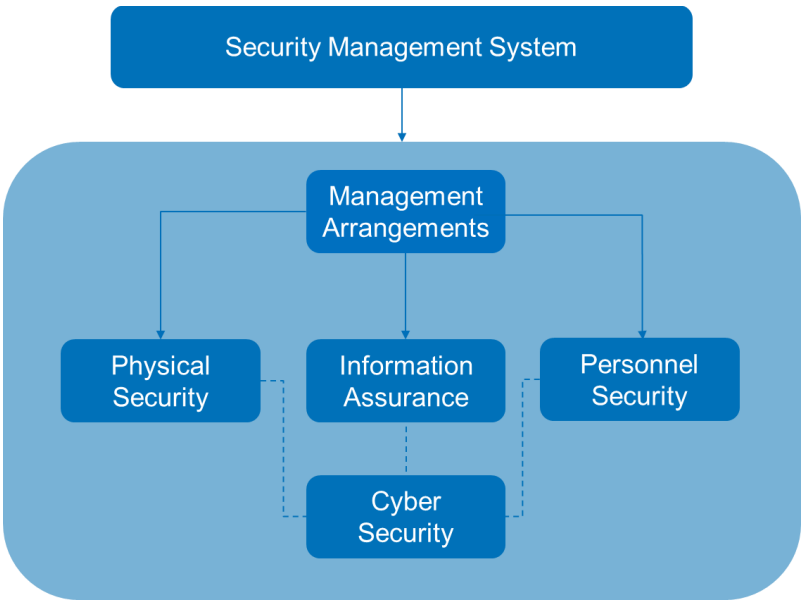

Figure 14: Key Elements of a Security Management System

The outcomes of the review were consolidated and subsequently used to develop a list of activities required to implement security management arrangements covering the following areas at the different IPR levels:

Table 3: Pathway Activities

Pathway Activities
(REDACTED)

A.2.3 GDA Step 1

(REDACTED)

[10] The physical security review included a review of the security arrangements at the designated List N facility.

A.2.4 GDA Step 2

(REDACTED)

A.2.5 Design Development Post GDA

(REDACTED)

A.3 Protection of Nuclear Material and SNI at a SMR-300 Site

(REDACTED)

- Key Security Plan Principles (KSyPP);
    - KSyPP 1 – Secure by Design
    - KSyPP 2 – The Threat
    - KSyPP 3 – The Graded Approach
    - KSyPP 4 – Defence in Depth
- Fundamental Security Principal (FSyP) and Security Delivery Principles (SyDP):
    - FSyP 6 – Physical Protection System
    - SyDP 6.1 – Categorisation for Theft
    - SyDP 6.2 – Categorisation for Sabotage
    - SyDP 6.3 – Physical Protection System Design
    - FSyP 7 – Cyber Security and Information Assurance
    - SyDP 7.1 – Effective Cyber and Information Risk Management
    - SyDP 7.3 – Protection of Nuclear Technology and Operations