Office for Nuclear Regulation

New Reactors Division – Generic Design Assessment

Step 4 Assessment of Security for the UK HPR1000 Reactor

Assessment Report ONR-NR-AR-21-010
Revision 0
January 2022

Published 01/22

For published documents, the electronic copy on the ONR website remains the most current publicly available version and copying or printing renders this document uncontrolled.

EXECUTIVE SUMMARY

This report presents the findings of my assessment of the security aspects of the UK HPR1000 reactor design undertaken as part of the Office for Nuclear Regulation's (ONR) Generic Design Assessment (GDA). My assessment was carried out using the Generic Security Report (GSR) and supporting documentation submitted by the Requesting Party (RP).

The objective of my assessment was to make a judgement, from a security perspective, on whether the generic UK HPR1000 design could be built and operated in Great Britain, in a way that is acceptably safe and secure (subject to site specific assessment and licensing), as an input into ONR's overall decision on whether to grant a Design Acceptance Confirmation (DAC).

The scope of my GDA assessment was to review the security aspects of the generic UK HPR1000 design by examining the claims, arguments and evidence in the security case. My GDA Step 4 assessment built upon the work undertaken in GDA Steps 2 and 3 and enabled a judgement to be made on the adequacy of the security information contained within the GSR and supporting documentation.

My assessment focused on the following aspects of the generic UK HPR1000 security case:

- The RP's submissions based on their GSR security case and supporting documents as they related to an application of selective Security Assessment Principles (SyAPs) and the adoption of a 'secure by design' approach drawing on the Key Security Plan Principles (KSyPPs).
- How the RP had carried out categorisation for theft and sabotage through the characterisation of their design. This included the methodology they had chosen based on Relevant Good Practice (RGP), its application against the design and a clear thread into the conceptual security regime.
- How the RP had carried out their characterisation of the design's technology as it related to cyber security risk. This involved the security of Nuclear Material (NM), Other Radiological Material (ORM) and Operational Technology (OT) together with the application of appropriate risk informed security controls. This included the methodology chosen based on RGP, its application against the design and a clear thread into the conceptual security regime.
- The RP's high-level SyAPs aligned security regime concept. I sought assurance that the RP's concept was underpinned by the results of both physical and cyber risk analysis. Also, that the RP had provided evidence that their case was aligned with a SyAPs-based 'outcomes' and indicative 'postures' approach to managing risk. Finally, that within their case, they had explained the conceptual security regime in sufficient and relevant detail so to inform a licensee in their formulation of a security plan at the site-specific stage.

The conclusions from my assessment are:

- The RP has produced a generic security infrastructure and architecture from 'first principles' against the UK Design Basis Threat (DBT). The RP has utilised UK expertise in doing this so to deliver a meaningful GDA.
- The RP has demonstrated that they have applied a SyAPs based approach. Specifically, that they have addressed adequately the KSyPPs. The RP has adopted and applied a 'secure by design' methodology. That requires the RP to identify security risks and address these through modifications. If modifications are not possible within GDA, the RP has made commitments for such mitigation to be considered in the site-specific stage. Where design changes cannot meet security expectations within GDA, or may not in the future, the RP

has developed a conceptual security framework to deliver a graded approach and one that offers adequate defence-in-depth to reflect the relative risk by location and magnitude.

- The RP has demonstrated that they have a workable methodology for assessing the risk posed by theft and sabotage against the UK HPR1000 generic design based on the UK DBT.
- The RP has captured the output from their risk analysis to inform a conceptual security regime that provides a licensee with a working framework to address KSyPPs. Also, they provided a framework by which a licensee could develop the concept further so to meet expectations regarding 'outcomes' and indicative 'postures' explained in a future security plan.
- The RP has also demonstrated that it has suitable risk assessment processes for evaluating the risks posed by malicious acts against Computer Based Systems Important to Safety (CBSIS) and has identified appropriate controls.
- The RP has demonstrated due diligence for Computer Based Security (CBSy) systems sufficiently to inform a licensee when installing a reasonably foreseeable security system commensurate with the relevant 'outcomes' stated in SyAPs.

These conclusions are based upon the following factors:

- A detailed and in-depth technical assessment, on a sampling basis, of the full scope of security submissions at all levels of the hierarchy of the generic UK HPR 1000 security case documentation.
- Detailed technical interactions on many occasions with the RP, alongside the assessment of the responses to Regulatory Queries (RQ) and Regulatory Observations (ROs) raised during the GDA.
- Independent information, reviews and analysis of key aspects of the cyber security case undertaken by a Technical Support Contractor (TSC).
- Detailed technical interactions on many occasions with the RP. Many alongside the ONR's lead Control & Instrumentation (C&I) inspector.

Several matters remain, which I judge are appropriate for a licensee to consider and take forward in its site-specific submissions. These matters do not undermine the generic UK HPR1000 design and security submissions but are primarily concerned with the provision of site-specific security case evidence which will become available as the project progresses through the detailed design, construction and commissioning stages. These matters have been captured in five Assessment Findings (AF).

Overall, based on my assessment, undertaken in accordance with ONR's procedures, the claims, arguments and evidence laid down within the GSR and supporting documentation submitted as part of the GDA process present an adequate security case for the generic UK HPR1000 design. I recommend that from a security perspective a DAC may be granted.

LIST OF ABBREVIATIONS

AACS	Automatic Access Control Systems
AF	Assessment Finding
APA	Adversarial Pathway Assessment
ARF	Airborne Release Fractions
BEIS	Department for Business, Energy and Industrial Strategy
BPX	Personnel Access Building
CAF	Cyber Assessment Framework
CAPSS	Cyber Assurance of Physical Security Systems
C&I (I&C)	Control and Instrumentation
CI&CS	Central Instrumentation and Control Systems
CAE	Claims-Arguments-Evidence
CBSIS	Computer Based Systems Important to Safety
CBSy	Computer Based Security
CCTV	Closed-Circuit Television
CGN	China General Nuclear Power Corporation Ltd
CIM	Communication Interface Modules
CNI	Critical National Infrastructure
CONOPs	Concept of Operations
CPNI	Centre for the Protection of National Infrastructure
CPPNM	Convention on the Physical Protection of Nuclear Material
CPA	Commercial Product Assurance
CPS	Cyber Protection System
CSDRS	Cyber Security Design Requirements Specification
CSRA	Cyber Security Risk Assessment
CSRAR	Cyber Security Risk Assessment Report
CS&IA	Cyber Security & Information Assurance
DA	Design Authority
DAC	Design Acceptance Confirmation
DBT	Design Basis Threat
DF	Decontamination Factors
DMGL	Delivery Management Group Lead
DRP (DR)	Design Reference Point
FCG	Fangchenggang Nuclear Power Plant
FSyP	Fundamental Security Principle
GDA	Generic Design Assessment
GNI	General Nuclear International Ltd.
GNSL	General Nuclear System Ltd.
GSR	Generic Security Report

HCVA	High Consequence Vital Area
HOW2	(ONR) Business Management System
HVM	Hostile Vehicle Mitigation
IAEA	International Atomic Energy Agency
ICBM	Independent Confidence Building Measures
IDS	Intrusion Detection System
IE	Initiating Event
IEMO	Initiating Event of Malicious Origin
IEC	International Electrotechnical Commission
ISAM	Independent Security Assurance Measures
ISO	International Organisation for Standardisation
JPO	(Regulators') Joint Programme Office
KSyPP	Key Security Plan Principles
LOOP	Loss Of Off-Site Power
MFES	Manual Forced Entry Standard
MCR	Main Control Room
MW	Megawatts
NCSC	National Cyber Security Centre
NM	Nuclear Material
NISR	Nuclear Industries Security Regulations 2003
NPP	Nuclear Power Plant
NSS	Nuclear Security Series
ONR	Office for Nuclear Regulation
ORM	Other Radiological Material
OT	Operational Technology
PAS	Publicly Available Specification
PCER	Pre-construction Environmental Report
PCSR	Pre-construction Safety Report
PPS	Physical Protection System
PSA	Probabilistic Safety Assessment
PSAS	Plant Standard Automation System
PWR	Pressurised Water Reactor
RCP (RCS)	Reactor Coolant Pump (Reactor Coolant System)
RF	Respirable Fraction
RGP	Relevant Good Practice
RHR	Residual Heat Removal
RI	Regulatory Issue
RO	Regulatory Observation
RP	Requesting Party

RPS	Reactor Protection System
RPV	Reactor Pressure Vessel
RSS	Remote Shutdown Station
RQ	Regulatory Query
SAP(s)	Safety Assessment Principle(s)
SA/SI	Security Architecture and Security Infrastructure
SCR	Security Control Room
SDS	System Design Specification
SEC	Sabotage Event Combination
SES	Sabotage End State
SNI	Sensitive Nuclear Information
STAR	Sabotage, Target Analysis and Review
SRS	System Requirements Specification
SOC	Security Operations Centre
SoDA	(Environment Agency's) Statement of Design Acceptability
SSC	Structures, Systems and Components
SyAP(s)	Security Assessment Principle(s)
SyDP	Security Delivery Principle
TAG	Technical Assessment Guide(s)
TSC	Technical Support Contractor
UK HMG	UK HM Government
UPS	Uninterruptable Power Supplies
URC	Unacceptable Radiological Consequence
VA	Vital Area
VAI	Vital Area Identification
VAI&C	Vital Area Identification & Categorisation
VPN	Virtual Private Network
WINS	World Institute for Nuclear Security

TABLE OF CONTENTS

Table(s)

Figure(s)

Annex(es)

1 INTRODUCTION

1.1 Background

1. This report presents my assessment conducted as part of the Office for Nuclear Regulation (ONR) Generic Design Assessment (GDA) for the generic UK HPR1000 design within the topic of Security.

2. The UK HPR1000 is a pressurised water reactor (PWR) design proposed for deployment in the UK. General Nuclear System Ltd (GNSL) is a UK-registered company that was established to implement the GDA on the UK HPR1000 design on behalf of three joint requesting parties (RP), i.e. China General Nuclear Power Corporation (CGN), EDF SA and General Nuclear International Ltd (GNI).

3. GDA is a process undertaken jointly by the ONR and the Environment Agency. Information on the GDA process is provided in a series of documents published on the joint regulators' website (www.onr.org.uk/new-reactors/index.htm). The outcome from the GDA process sought by the RP is a Design Acceptance Confirmation (DAC) from ONR and a Statement of Design Acceptability (SoDA) from the Environment Agency.

4. The GDA for the generic UK HPR1000 design followed a step-wise approach in a claims, argument and evidence hierarchy which commenced in 2017. Major technical interactions started in Step 2 which focused on an examination of the main claims made by the RP for the UK HPR1000. In Step 3, the arguments which underpin those claims were examined. The Step 2 reports for individual technical areas, and the summary reports for Steps 2 and 3 are published on the joint regulators' website. The objective of Step 4 was to complete an in-depth assessment of the evidence presented by the RP to support and form the basis of the safety and security cases.

5. The full range of items that form part of my assessment is provided in ONR's GDA Guidance to Requesting Parties (Ref. 1). These include:

   - Consideration of issues identified during the earlier Step 2 and 3 assessments.
   - Judging the design against the Security Assessment Principles (SyAPs) (Ref. 2) and whether the proposed design ensures risks are understood, reduced or removed through modifications, and that any consequential mitigation meets expectations within SyAPs.
   - Assessing arrangements for ensuring that security claims and assumptions will be realised in the final as-built design.
   - Assessing the arrangements for developing the GSR into a site security plan.
   - Resolution of identified nuclear security issues or identifying paths for resolution.

6. The purpose of this report is therefore to summarise my assessment in the security topic which provides an input to the ONR decision on whether to grant a DAC, or otherwise. This assessment was focused on the submissions made by the RP throughout GDA, including those provided in response to the Regulatory Queries (RQs) and Regulatory Observations (ROs) I raised. Any ROs issued to the RP are published on the GDA's joint regulators' website, together with the corresponding resolution plans.

1.2 Scope of this Report

7. This report presents the findings of my assessment of the security of the generic UK HPR1000 design undertaken as part of GDA. I carried out my assessment using the Generic Security Report (GSR) (Ref. 3) and supporting documentation submitted by the RP. My assessment was focused on considering whether the generic security case

provides an adequate justification for the generic UK HPR1000 design, in line with the objectives for GDA.

1.3 Methodology

8. The methodology for my assessment follows ONR's guidance on the mechanics of assessment, NS-TAST-GD-096 (Ref. 4).

9. My assessment was undertaken in accordance with the requirements of ONR's HOW2 Business Management System. ONR's Security Assessment Principles (SyAPs) (Ref. 2), together with supporting Technical Assessment Guides (TAG) (Ref. 4), were used as the basis for my assessment. Further details are provided in Section 2. The outputs from my assessment are consistent with ONR's GDA Guidance to RPs (Ref. 1).

2 ASSESSMENT STRATEGY

10. The strategy for my assessment of the security aspects of the UK HPR1000 design and security case is set out in this section. This identifies the scope of the assessment and the standards and criteria that have been applied.

2.1 Assessment Scope

11. A detailed description of my approach to this assessment can be found in the security assessment plan (Ref. 5). Also, to support my integration with the Control & Instrumentation (C&I) topic, a cyber security assessment strategy was also captured as a specific assessment plan (Ref. 6). The overall scope of this assessment was bound by the RP's declared scope for the UK HPR1000 GDA Project (Ref. 4).

12. I considered all the main submissions within the remit of my assessment scope, to various degrees of breadth and depth. I chose to concentrate my assessment on those aspects that I judged to have the greatest security significance. My assessment was also influenced by the claims made by the RP, my previous experience of similar systems for reactors and other nuclear facilities, and any identified gaps in the original submissions made by the RP. A particular focus of my assessment has been the RQs and an RO I raised because of my on-going assessment, and the resolution thereof.

2.2 Sampling Strategy

13. In line with ONR's guidance (Ref. 4), I chose a sample of the RP's submissions to undertake my assessment. I sought evidence that the RP had acknowledged that security is at the conceptual design stage during GDA therefore would need to be developed from 'first principles'. Moreover, that the GSR set the conditions for a licensee to develop it further into a site security plan.

14. First, I sought evidence of the RP taking a SyAPs based approach. This is the first GDA to be fully assessed against SyAPs. Then I focused on the most relevant principles and the RP choice of security risk-based methodologies. Thereafter, their application of that risk analysis to inform a high-level security regime concept. I accepted that a full site security regime would be developed by the licensee.

15. Then I sought evidence that the RP had taken a 'secure by design' approach within a broader application of the Key Security Plan Principles (KSyPPs). Further to 'secure by design' (KSyPP 1), I sought evidence of the use of the UK Design Basis Threat (UK DBT) at KSyPP 2, the application of a 'graded approach' (KSyPP 3), then for the RP's case to have described sufficient 'defence in depth' (KSyPP 4). Thereafter, how they had described their security regime using functions and systems categorisation (KSyPP 5), referencing codes and standards (KSyPP 6) where applicable. As part of a 'secure by design' approach, I sought evidence of the RP having conducted modifications to the design or, if not, to have made commitments for a licensee to consider.

16. Focusing on risk analysis and chosen methodologies, I sought evidence of the use of Relevant Good Practice (RGP) both in the RP's choice of methodology and then its application in terms of categorisation for theft and sabotage against the design. Likewise, I sought evidence of the application of RGP in terms of assessing the risk posed by cyber-related malicious acts against equipment and software used in activities that would involve Nuclear Material (NM), Other Radioactive Material (ORM) and Computer Based Systems Important to Safety (CBSIS).

17. Having considered the RP's security risk analysis with regards to both physical and cyber threats, and against the UK DBT, I sought evidence that it had informed and shaped their conceptual security regime. Moreover, that the product provided a

suitable framework for a licensee to develop a security plan. Also, that residual cyber risks and related requirements management for the licensee had been captured adequately. I then sought evidence that the RP's generic security concept should be sufficient to provide a licensee with a working framework to achieve the KSyPPs and be suitably aligned with SyAPs-based specified 'outcomes' and indicative 'postures' (details of which are not mentioned here and are SNI) in sufficient detail to inform a future security plan. As security arrangements must be deconflicted with aspects of safety, I expected the RP to have in place a means to manage cross-cutting issues within the scope of GDA. I therefore focused on the RP's modifications process and its application.

18. While acknowledging that a licensee would develop a security infrastructure to meet the prevailing threat, I sought evidence that the RP had considered future security systems and their protection in terms of Computer Based Security (CBSy). I acknowledged that such detailed design of security systems would be for the site-specific stage of development. Choices for a future security systems architecture, with its networks and specific capabilities such as detection systems, is for the licensee to decide and develop. Nonetheless, I sought evidence that the RP had considered the implications for a reasonably foreseeable security system architecture.

2.3 Out of Scope Items

19. The following items were outside the scope of my assessment as declared by the RP in the UK HPR1000 GDA Project (Ref. 7).

- Information technology systems to hold future Sensitive Nuclear Information (SNI.)
- Information security for the RP as it relates to Regulation 22 of the Nuclear Industries Security Regulations (NISR) 2003. This is an enabling activity for GDA and is regulated outside of this assessment.

2.4 Standards and Criteria

20. The relevant standards and criteria adopted within this assessment are principally the SyAPs (Ref. 2), TAGs (Ref. 4), relevant national and international standards and Relevant Good Practice (RGP) informed from existing practices adopted on nuclear licensed sites. The key SyAPs and any relevant TAGs, national and international standards and guidance are detailed within this section. RGP, where applicable, is cited within the body of the assessment.

2.4.1 Security Assessment Principles

21. The SyAPs (Ref. 2) constitute the regulatory principles against which ONR judge the adequacy of security cases. The SyAPs pertinent to GDA are included within Annex 1 of this report. While SyAPs are applicable to assessments of plant designs within GDA, the document is written to enable ONR to assess developed nuclear premises so that security arrangements, detailed within an approved security plan, meet regulatory expectations. Within GDA, the RP is not able to produce a security plan that would demonstrate how security outcomes would be achieved. However, the RP's conceptual security regime should inform a licensee when producing such detailed plans.

22. The key SyAPs applied within my assessment were the KSyPPs together with Fundamental Principles 6 and 7. These I judged as being most aligned with assessing designs within the scope of GDA.

23. Given the complementary relationship between safety and security, ONR Safety Assessment Principles (SAPs) (Ref. 8) include guidance on how to assess security related matters where these fall within the vires of safety legislation because of an

overlap of interest. Where SAPs are applied as part of this assessment, a justification has been provided within the relevant section of this report.

2.4.2 Technical Assessment Guides

24. The following TAGs were used selectively as part of this assessment (Ref. 4):

- GNS-TAST-GD-6.1, Categorisation for Theft
- GNS-TAST-GD-6.2, Categorisation for Sabotage
- GNS-TAST-GD-6.3, Physical Protection System Design
- GNS-TAST-GD-7.1, Effective Cyber and Information Risk Management
- GNS-TAST-GD-7.3, Protection of Nuclear Technology and Operations
- GNS-TAST-GD-7.5, Preparation for and Response to Cyber Security Incidents
- GNS-TAST-GD-11.1, Guidance on the Security Assessment of Generic New Nuclear Reactor Designs

2.4.3 National and International Standards and Guidance

25. The following standards and guidance were used as part of this assessment:

- International Atomic Energy Agency (IAEA) Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5). (Ref. 9).
- The UK DBT. (Ref. 10).
- IAEA Technical Guidance document (NSS No 16) 'Identification of Vital Areas at Nuclear Facilities'. (Ref. 9).
- The National Cyber Security Centre standards, guidance, and principles documents. (Ref. 11).
- IAEA Computer Security of Instrumentation and Control Systems at Nuclear Facilities. Nuclear Security Series No. 33-T. (Ref. 9).
- IEC standards 27005, 62645, 62443. (Ref. 12).

2.5 Use of Technical Support Contractors

26. It is usual in GDA for ONR to use Technical Support Contractors (TSCs) to provide access to independent advice and experience, analysis techniques and models, and to enable ONR's inspectors to focus on decision making.

27. Table 1, below, sets out the areas in which I used a TSC to inform my assessment. I required this support to assist me when working with the C&I assessors. The TSC was able to provide both C&I and cyber security expertise.

Table 1: Work Packages Undertaken by the TSC

Number	Description
1	This TSC work specification was submitted by the lead C&I assessor. As part of the work conducted under the C&I specification, the CS&IA assessor asked the TSC to report on a specific area. This was specifically regarding relevant threat actors and associated sabotage actions. (Contract number ONR-604)

28. The TSC undertook detailed technical reviews, and this was conducted under my supervision. The regulatory judgment on the adequacy, or otherwise, of the generic UK HPR1000 safety and security case in this report has been made exclusively by ONR.

2.6 Integration with Other Assessment Topics

29. GDA requires the submission of an adequate, coherent and holistic generic security case. Regulatory assessment cannot be carried out in isolation as there are often issues that span multiple disciplines. Consequently, I have worked closely with several other ONR inspectors so to inform my assessment. The key interactions were:

- Fault Studies to inform the assessment of the RP's Vital Area Identification and Categorisation (VAI&C) analysis. The UK HPR1000 fault schedule and associated references were a key input to this work.
- A radiological consequence specialist inspector provided support in determining the adequacy and accuracy of the RP's radiological dose consequence methodology, its calculations, and subsequent results.
- C&I, by working jointly with inspectors to ensure the cyber risk to Operational Technology (OT), and specifically reactor protection systems, have been addressed holistically by the RP.
- Fire Safety to ensure deconfliction of evacuation routes and access through security vulnerable areas have been considered.
- Human Factors in seeking assurance that in achieving the requisite security measures, the RP did not unintentionally degrade critical safety functions and related measures, although this aspect will be more relevant in detailed design.
- Electrical Engineering regarding power to security systems although this requirement will be managed later in detailed design.

3 REQUESTING PARTY'S SECURITY CASE

3.1 Introduction to the Generic UK HPR1000 Design

30. The generic UK HPR1000 design is described in detail in the Pre-Construction Safety Report (PCSR) (Ref. 13). It is a three-loop PWR designed by CGN using the Chinese Hualong technology. The generic UK HPR1000 design has evolved from reactors which have been constructed and operated in China since the late 1980s, including the M310 design used at Daya Bay and Ling'ao (Units 1 and 2), the CPR1000, the CPR1000^{+} and the more recent ACPR1000. The first two units of CGN's HPR1000, Fangchenggang (FCG) Nuclear Power Plant (NPP) Units 3 and 4, are under construction in China and Unit 3 is the reference plant for the design. The design is claimed to have a lifetime of at least 60 years and has a nominal electric output of 1,180 MW.

31. The reactor core of the UK HPR1000 design contains zirconium clad uranium dioxide (UO_2) fuel assemblies and reactivity is controlled by a combination of control rods, soluble boron in the coolant and burnable poisons within the fuel. The core is contained within a steel Reactor Pressure Vessel (RPV) which is connected to the key primary circuit components, including the Reactor Coolant Pumps (RCP), Steam Generators (SGs), pressuriser and associated piping, in the three-loop configuration. The design also includes a number of auxiliary systems that allow normal operation of the plant, as well as active and passive safety systems to provide protection in the case of faults, all contained within a number of dedicated buildings.

32. The reactor building houses the reactor and primary circuit and is based on a double-walled containment with a large free volume. Three separate safeguard buildings surround the reactor building and house key safety systems and the main control room. The fuel building is also adjacent to the reactor and contains the fuel handling and short term storage facilities. Finally, the nuclear auxiliary building contains a number of systems that support the operation of the reactor. In combination with the diesel, personnel access and equipment access buildings, these constitute the nuclear island for the generic UK HPR1000 design.

3.2 The Generic UK HPR1000 Security Case

33. The RP's GSR is their security case and is captured within a hierarchy of documents (at Figure 1). Reflecting security RGP, the security case explains a 'golden thread' that starts with the design, identifies security risks, assesses their magnitude in terms of impact and seeks to reduce vulnerabilities or, if this is not feasible, offer ways and means mitigate them in detail design. The RP's case therefore seeks to design-out identified security risks and vulnerabilities, identified throughout various design changes and captured through modifications. If such risk reduction cannot be fully achieved within GDA through such modifications, then the case goes on to explain where protective security could be designed-in to protect the plant at a later stage of development. Therefore, the RP's case follows the objectives of a 'secure by design' methodology. More generally, they have adopted an approach that follows the logic explained within the KSyPPs, together with the relevant FSyPs. As the reference design security arrangements were not predicated on the UK DBT, and related regulatory expectations, the RP has developed its case from 'first principles'. As the design has evolved through GDA, the RP has set Design Reference Points (DRP). My assessment has been against DR 2.2 and consolidated at the end of GDA against DR 3.

34. At the top of their hierarchy is their 'header' document, referred to as the GSR security case at Tier 1. That document provides an overview of the generic security case for the UK HPR1000. It also offers a road map of submissions, designated as Tier 2 and 3, and how they inform the RP's high-level security concept. By way of a summary, the

RP has aimed to demonstrate how it meets the expectations within SyAPs but also drawing on other RGP. In accordance with a goal-setting regulatory regime, the RP has provided explanations of how it has addressed specified 'outcomes' and indicative 'postures' within SyAPs.

35. At Tier 2, the RP's security team provided detail of their methodologies for risk assessment and applied these against the UK HPR1000 design that informed their conceptual security regime. Further analysis is provided in the Tier 3 documents. In developing their 'golden thread', the RP extracted the relevant security information from the Design and Plant Information document (Ref. 14). That document provided details of general plant information for those facilities within scope of the GDA assessment. The document provided them with the necessary detail on the design, its layout and main building configuration. It informed them of the nuclear inventory with the potential to cause significant off-site radiological consequences. It also provided detail of the fundamental safety functions necessary to keep the plant in a safe condition, the related Instrumentation and Control (I&C) systems that deliver safety functions and various operating modes. That information also provided the detailed data to undertake a security characterisation of that design so to determine the categorisation for theft based on the quantities and forms of Nuclear Material (NM) and Other Radiological Material (ORM) held within the buildings in scope.

36. The RP applied the UK DBT (Ref. 10), and this was explained within its Threat Interpretation document (Ref. 15). This document defined the physical and cyber threats that they intended to apply to the UK HPR1000 design. The document reflected the UK DBT (Ref. 10) and has drawn from other RGP regarding the cyber threat. Some of that RGP included ONR's UK Civil Nuclear Sector Cyber Threat Assessment (Ref. 16).

37. The RP selected, developed, and then applied its VAI (and thereafter categorisation) methodology to the design. That procedure, captured in their VAI&C methodology document (Ref. 17), included the application of the UK DBT to the design, reflected and developed RGP and was adapted to meet the needs of GDA. The RP methodology was broken down into phases and included a means by which to carry out categorisation, commensurate to the level of design developed during GDA, so to inform a 'graded approach'. Their analysis, drawn from the safety case and with supporting drawings, was included in the VAI&C Report (Ref. 18) with its numerous supporting annexes. These annexes provided the detail of locations, threats, the nuclear inventory and the analysis from applying their methodology including categorisation. The report also identified several modifications. One annex is dedicated to theft analysis. Further detailed analysis was captured in related Tier 3 documents. That work then provided the detail of what to protect and why, locations by rooms, floors and buildings and calculated radiological consequences should a sabotage scenario be successful. In this analysis, the RP described how the identification of 'direct' and 'in combination' vital areas would inform a 'graded approach'. Also, they designated specific locations and related sabotage scenarios as either Vital Areas (VA) or High Consequence Vital Areas (HCVA), again to reflect a 'graded approach'.

38. The RP also carried out a similar process for cyber risks working closely with their C&I colleagues. They first produced a methodology, the Cyber Security Risk Assessment Methodology (Ref. 19), as the process to assess the cyber security risks to the UK HPR1000 generic design. This was explained in seven steps, including potential design vulnerabilities, leading to Cyber Protection System (CPS) 'outcomes' and control sets (based on international standards) together with a residual risk assessment and related remedial measures. The Tier 2 document, the Cyber Security Risk Assessment Report (CSRAR) (Ref. 20), captured the output of their analysis. Their focus was primarily CBSIS as this affects security risks that are exploited by threat actors informed by the UK DBT. The RP acknowledged Computer Based Security Systems (CBSy) although explained that this aspect of their conceptual

design would be for a licensee to further develop. Likewise, certain CBSIS control sets have been identified as to be implemented post GDA. What is often called business information technology, is outside GDA scope and for a licensee to consider. The analysis presented in the RP's Tier 2 and Tier 3 documents informed their high-level security regime concept.

39. The output from the analysis of all relevant security risks and managing their consequences is captured in the Security Architecture and Security Infrastructure (SA/SI) (Ref. 21) and Concept of Operations (CONOPs) (Ref. 22) documents. These documents explain how, within the scope of GDA, the RP applies the KSyPPs. Specifically, how they have applied a 'secure by design' approach. These documents describe the conceptual security design based on their analysis of the risks and categorising them so to apply a 'graded approach'. They also inform the achievement of 'defence in depth'. The RP's high-level security concept is a framework by which the licensee might build a security case and security plan. That framework is structured around the KSyPPs and applies protection functions such as detection and delay to the plant design. The RP explains generic security capabilities, such as CCTV, to illustrate how a licensee could meet the security functions that are captured within SyAPs, again reflecting broader RGP. Modifications and post GDA commitments are captured in the CONOPs document.

40. The CONOPs document completes the 'golden thread' of the RP's security case. That is the logical process of describing aspects of the plant, the inherent risks, their risk analysis and how such identified vulnerabilities receive proportionate protection.

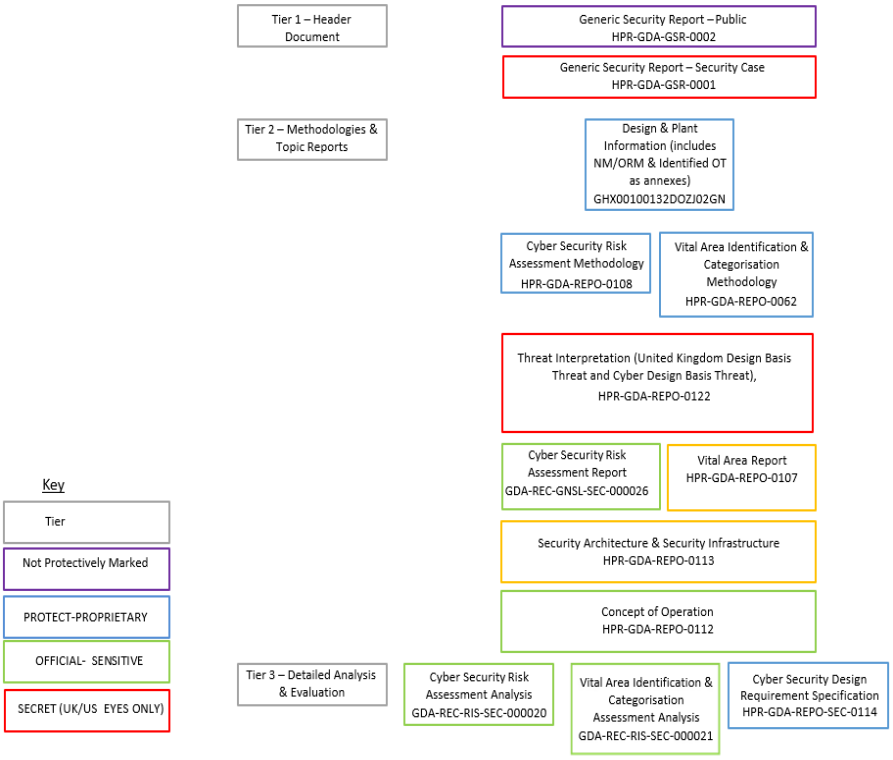

Figure 1 – UK HPR1000 Generic Security Case Structure

4 ONR ASSESSMENT

4.1 Structure of Assessment Undertaken

41. PCSR Chapter 27, (Ref. 13), provides an outline of the RP's approach to delivering the GSR. The RP described the structure of its documentation, RGP to be used and explained its methodologies to assess security risk. The submissions, that provided the basis for my assessment, were drawn from Chapter 27. These key documents, that provide the 'golden thread' from security risk analysis to a conceptual high-level security design, were reviewed and developed throughout GDA and provided the basis for my final assessment.

42. My assessment is specified in my Assessment Plan for Step 4 (Ref. 5) and is a continuation of the topics within Steps 2 and 3. The topics chosen were consistent with specific aspects of SyAPs (Ref. 2) that are germane to GDA. For GDA, my assessment has been based on the RP's understanding of the plant, security risks and how they might be designed-out or reduced and, if not, how they would be addressed by way of a security conceptual design for both cyber and physical risks. This work is best described as 'secure by design' with the expectation that the RP has drawn from KSyPPs and selected SyAPs.

43. The RP introduced the key security topics in the earlier stages of GDA with their methodologies assessed in Steps 2 and 3 before their application in Step 4. However, both the vital area and cyber security risk methodologies have been updated through experience and improved in Step 4. For instance, the vital area categorisation methodology has been developed further by the RP. The outputs from applying the RP's risk-based methodologies have been the focus of my assessment in Step 4.

44. In terms of the culmination of GDA, I have assessed the GSR security case (Tier 1). This is the RP's high-level 'header' document that summarises its approach to security risks and findings in terms of 'secure by design'. This report is designed to be read as a 'standalone' document that should demonstrate a nuanced application of selective SyAPs.

45. While the Tier 1 document is a summary, most of my assessment has been of the Tier 2 and selected Tier 3 documents. The first, and major aspect of GDA, was to assess the RP's vital area and cyber security risk analysis and the output. Their categorisation for theft and sabotage through the characterisation of the design in scope, I considered a key deliverable for assessment and was my focus for Step 4. Aligned with vital area work, my assessment included design technology as it related to 'cyber' security risk. Importantly, in this GDA, I sought evidence that both cyber and physical threats were addressed 'holistically', and their analysis captured in an integrated security conceptual solution that would inform the licensee.

46. A key aspect of the RP's security case was its SyAPs-aligned high level conceptual security regime. I sought evidence that the regime was suitably underpinned by the results of both physical and cyber risk analysis. Moreover, that they had explained how their regime, in framework form, would address security system SyAPs 'outcomes' and indicative 'postures' thereby setting the conditions for the licensee to produce a credible security case and plan.

47. Reflecting my Step 4 assessment plan (Ref. 5), my detailed assessment is captured in the subsequent sections that follow logically from the RP's security case, vital area and cyber security risk analysis, the product of such analysis and how that has informed the high-level security concept. Moreover, that the generic concept for security has sufficient utility for the licensee so it might translate into a security plan for the plant 'end-state'.

4.2 Generic Security Report – Security Case

4.2.1 Assessment

48. The GSR (Ref. 3) is the RP's security case and is explained initially within its Tier 1 document. This document provides a summary of the RP's approach to the security aspects of GDA. It explains the purpose and objectives of the GSR. Moreover, it describes how the RP had taken an approach that was aligned to SyAPs. The RP acknowledged that for the scope of GDA, the balance of a nuclear site considered in the site-specific phase of the project would also include security infrastructure that would contribute to meeting the 'outcomes' stipulated within SyAPs. This Tier 1 document also provides a guide to navigating their Tier 2 and 3 documents that explain the methodology used to identify and categorise risks and their mitigation, all necessary for a meaningful GDA. My intention with this topic was to assess whether this 'header' document captured the key elements of a security GDA accepting that the arguments and evidence relating to security risks would be in the Tier 2 and 3 documents and the focus for my assessment. I judged these key elements of security to be an understanding of the plant in scope, identified security risks and their mitigation through applying a 'secure by design' approach. I did not expect the Tier 1 document to go into detail. Also, I expected that this report could be read as a standalone document albeit one that would be published with other material captured in classified annexes. Principally, I assessed whether this document set the scene for a licensee to develop their security case and plan for the site-specific stage. I also looked for coherence with the Tier 2 and 3 submissions and that there was sufficient signposting from this document into the evidence at lower tiers.

49. Reflecting the assessment plan for Step 4 (Ref. 5), I have used elements of SyAPs to inform my judgements. Explicitly, I have drawn from KSyPPs as they are most germane to GDA. Specific to GDA is the GDA TAG. The Security GDA TAG (CNS-TAST-GD-11.1 Rev 0) (Ref. 4) provides specific guidance on assessing RP submissions and has been used throughout GDA. However, to capture additional security thinking, I shared with the RP my additional note for GDA (Ref. 23). That note highlighted the need for security to be embedded within the modification process reflecting IAEA guidance (Ref. 9). As these guides, and their regulatory expectations, inform the assessment of future security cases and plans they are germane to GDA. I expected the RP to use this RGP and draw from wider sources including operational experience.

50. With an expectation that the RP would develop this Tier 1 document throughout GDA, I provided feedback on the GSR Version 1 (Ref. 24). With Version 1, I informed the RP that it was comprehensive and easy to follow. However, I offered the RP advice on areas that might be strengthened to explain how they had applied a 'secure by design' approach in meeting the expectations within SyAPs as they are relevant to GDA.

51. In Step 4, I sought further reassurance that the document had matured so to meet expectations in terms of its value and purpose at the close of GDA. Consequently, in Step 4 the RP provided an update on the development of the GSR. This update would be consistent with DR 3. The RP provided an updated document layout (Ref. 25) and a 'Change Log' (Ref. 26). The latter explained how the security case would be updated drawing from my feedback at workshops, ROs, RQs, modifications, commitments and changes to Tier 2 documents. Later in Step 4, the RP provided further detail on the content of Version 2 (Ref. 27). Once again, this material provided further evidence of the development of this Tier 1 document that met my expectations for GDA.

52. Therefore, based on the Change Log, briefings and submitted extracts, I am content that Version 2 meets my broad expectations for GDA. This is because my main effort has been on the detail within Tier 2 documents substantiated in some Tier 3 submissions.

53. Specifically, I am content that the areas for improvement have been captured and explained in the Change Log. This is because the RP's work on the cyber security risk assessment has matured significantly together with their conceptual security regime. Similarly, the RP has examined and explained how SyAPs 'outcomes' and 'postures' together with security functions are used in their conceptual design framework. These have been applied extensively in the SA/SI document that is assessed in later sections of my report. Therefore, I am content that the case is sufficiently aligned with SyAPs, and the expectations outlined in the regulatory assessment of security plans, thereby meeting my expectations and providing a suitable framework for a licensee to develop.

54. With opportunities to apply a 'secure by design' approach within the GDA process, given its focus on the design stage, the RP has now developed both its methodology and application based on the modification process and change control procedures. This has been explained in detail in their SA/SI and CONOPs documents and now suitably summarised in the GSR Tier 1 document. The RP captures this idea under a new section on 'holistic security' that describes the 'golden thread' from design to protection thereby meeting my expectations.

55. I previously advised that the RP should integrate cyber into its GSR, to avoid having it as a separate topic. In that way the product might be described as 'holistic'. I consider that the RP has addressed cyber security risk analysis and its mitigation in sufficient detail within this Tier 1 document. Detailed assessment of these specific topics is covered later in this report.

4.2.2 Strengths

56. The RP has drawn on RGP and provided a mature explanation of the security case within this Tier 1 document. The document highlights a number of important security themes and they have developed these intelligently. For example, they refer to the idea of 'holistic security' by which they have brought cyber and physical risk management together and adopted, then developed, a 'secure by design' methodology. The RP has taken a progressive approach and used the KSyPPs to outline a case that has utility for the licensee. The GSR Tier 1 document is a more comprehensive explanation of the 'golden thread' and has sufficient detail to be read as a standalone summary of the RP's security case for the generic UK HPR1000 design during GDA.

4.2.3 Outcome

57. I have raised no Assessment Findings (AF) from this part of my assessment.

4.2.4 Conclusion

58. Based on the outcome of my assessment of the GSR Tier 1 document, I conclude that it meets my expectations. The document captures the main themes from SyAPs as they relate to GDA. The RP has developed these themes, that are part of evolving RGP, intelligently and in sufficient detail. Specifically, they have taken a holistic approach by bringing together the physical and cyber elements of a security risk analysis.

4.3 Vital Area Identification and Categorisation

4.3.1 Background

59. This section presents the assessment of the UK HPR1000 GDA VAI&C submissions presented by the RP.

60. VAI&C is the process of identifying critical infrastructure within a nuclear site or facility which must be protected to prevent or reduce the likelihood of an off-site dose that

would endanger public health by exposure to radiation that would be judged as unacceptable. This is referred to as an 'Unacceptable Radiological Consequence' (URC) as defined by UK HMG.

61. VAI&C is used to define a boundary around key Systems, Structures or Components (SSC) or NM to ensure they are provided with a proportionate level of security protection. Protection levels are categorised as baseline, a VA or a HCVA in accordance with Annex B of the SyAPs (Ref. 2). This categorisation is then used to inform the protective security design 'outcomes' in accordance with Security Delivery Principle (SyDP) 6.3.

62. To ensure that protection systems provide an appropriate level of defence, they should be designed, evaluated and tested using the UK DBT (Ref. 10). The custodian of the UK DBT is the UK HMG and its risk appetite in applying the UK DBT is based on a probability of one. In the context of VAI&C this means that all threats are applicable, and all can be realised in any combination.

4.3.2 Assessment Scope and Sampling Approach

63. I chose to consider the RP's entire VAI&C document set to inform my regulatory judgements. My assessment has focused on the claims, arguments and evidence with the emphasis being on the Tier 3 documents. These documents provide the evidence to substantiate the arguments made in Tier 2 which link back to the claims made in the Tier 1 document. The RP's claim, that has been the target of my assessment, is:

- The security threat will be managed to protect the public from the risks arising from a radiological event caused by the theft or sabotage of nuclear or other radioactive material and supporting systems.

64. This claim aligns with the RGP set out in SyDP 6.2 (Categorisation for Sabotage) which states the dutyholder should undertake a characterisation of their site and facilities to determine the categorisation for sabotage.

65. My focus has been on assessing the intent of the RP's VAI&C submission for the UK HPR1000 to demonstrate that the following outcomes have been achieved:

- Identification of the nuclear inventory within the scope of GDA including its specific location within the nuclear island.
- Identification of the SSCs requiring protection to prevent the sabotage and theft of the nuclear inventory together with their locations and potential sabotage combinations.
- Identification and location of the C&I technology that could facilitate the sabotage of the assets through a cyber threat.
- Development and application of a dedicated UK HPR1000 GDA threat interpretation document, consistent with the requirements of the UK DBT.
- Implementation of the 'secure by design' principle to facilitate the identification of design modifications to eliminate or reduce the potential for sabotage and theft.
- Development of a list of plant areas for protection against theft and sabotage which have been suitably categorised.

66. The main documentation that formed the basis for my assessment was:

- The VAI&C methodology (Ref. 17) that presents the RP's processes and procedures within a five-step process.
- VAI&C analysis document (Ref. 18) that provides an overview of the complete document set signposting the links between the claims, arguments and

evidence in a tabulated format. The document is supported by eight Tier 3 annexes which provide the necessary evidence.

- The nuclear inventory (Ref. 28) that presents details of the UK HPR1000's NM/ORM.
- Their assessment of the inventory (Ref. 29) to determine the worst-case potential for the release of a URC if the inventory is sabotaged.
- Their identification of Initiating Events of Malicious Origin (IEMO) and Potential Sabotage Event Combinations (SEC) (Ref. 30) that present the potential targets for protection from sabotage and sabotage events which could lead to a URC.
- Their location analysis (Ref. 31) that presents the locations of potential targets.
- The threat assessment document (Ref. 32) to determine those potential sabotage event combinations which can be considered to be credible, based on the capabilities of the threat. Representative Sabotage End States (SES) are then declared that describe the condition of the SSC following a malicious attack.
- Their assessment of theft (Ref. 33) that presents the categorisation of the NM/ORM inventory for theft. It identifies the materials and their locations that require protection.
- VAI&C (Ref. 34) that presents the output of the overall assessment and identifies the areas requiring protection against sabotage. These are categorised based on the magnitude of their URC potential in accordance with SyAPs.
- Their Basis of Assessment document (Ref. 35) that presents a record of the key information sources and supporting references.

4.3.3 Assessment

67. During the late stages of Step 3 the RP submitted a revision of its HPR1000 VAI&C study, the ONR GDA Step 3 assessment (Ref. 36) provides further detail. My assessment of this submission identified a number of shortfalls in meeting regulatory expectations. These shortfalls generally related to the adequacy of the RP's underpinning arrangements and methodology for VAI&C. In my judgement, at the early stages of any safety or security driven process, it is essential that the methodology to deliver the desired outcome is well established, tested, proven and then adequately implemented. Therefore, my focus was for the RP to develop its arrangements for VAI&C and then to ensure that those arrangements had been adequately implemented and adjusted according to learning through their application and any design modifications. In order to achieve the above outcome, I raised RO-UKHPR1000-0025 (Ref. 37).

68. The intent of the RO was for the RP to develop adequate written arrangements for VAI&C, to implement those arrangements and present a VAI&C study commensurate with the design information available at DR2.2 for all reactor operating states as detailed below.

Table 2 – Reactor operating states

Operating state	Description
State A	Power states, hot and intermediate shutdown states
State B	Intermediate shutdown with temperature above 140^0C
State C	Intermediate shutdown and cold shutdown conditions under Residual Heat Removal (RHR) operation mode

Operating state	Description
State D	Cold shutdown
State E	Cold shutdown during refuelling
State F	Cold shutdown when the fuel fully unloaded

69. In response, the RP updated its VAI&C methodology and submitted a revision to ONR for assessment (Ref. 38). In addition, the RP submitted its Vital Area Report for plant operating State A (Ref. 39).

70. At a high level I judge that the RP's revised methodology offers a structured approach for the assessment of sabotage for the UK HPR1000. This is because their approach is centred on the asset requiring protection, the NM or ORM with URC potential, and then adopts safety analysis to determine the means by which the plant may be sabotaged in order to generate a URC.

71. The RP's VAI&C methodology consisted of a five-phased approach. The documentation, forming the VAI submission that supports each of the five phases, has been subjected to a detailed assessment. My judgements are set out below against each phase in turn.

Phase 1: Analysis of NM/ORM Inventory.

72. The RP's intent in Phase 1 was to identify and categorise the NM/ORM in terms of form, quantity, activity and location within the plant during each plant operating state. The outcome of Phase 1 is captured in DR2.2 Annex A (Ref. 28) and Annex B (Ref. 29) which present the supporting evidence for Phase 1.

73. Annex A presents the evidence to support the following arguments:

- The nuclear inventory is based on currently available information for the UK HPR1000 design.
- The nuclear inventory considers form, location, activity and quantity of the NM/ORM as well as potential changes during the project lifecycle.

74. The inventory, detailed in Annex A, is based upon the single-unit UK HPR1000 design which is consistent with the scope of GDA and uses the latest available information at DR2.2. The document contains a list of all significant sources of NM, comprising fissionable material, and ORM located within the extant UK HPR1000 design. Having assessed the content of Annex A, I am satisfied that sufficient detail has been presented, commensurate with the inventory data available at DR2.2, to support the VAI&C analysis. The inventory is categorised in terms of its form, type, location, quantity and variation during the plant lifecycle which is consistent with RGP (Ref. 4) and meets my expectations for Step 4 of the UK HPR1000 GDA.

75. Annex B presents the evidence to support the following arguments:

- The assessment of the URC potential of NM/ORM has been undertaken on a conservative basis using available information.
- Appropriate radiological dose levels for URC assessment have been applied.

76. This annex analyses the inventory identified in Annex A to determine its potential to create a URC as a result of sabotage. The analysis carried out at this stage is done on a highly conservative basis using a dose calculation formula which has Airborne

Release Fractions (ARF), Respirable Fractions (RF) and Decontamination Factors (DF) set to unity to represent a totally vaporised, respirable release with no restriction to its spread to the site boundary. This stage of the analysis is based on the following conservative assumptions:

- As no site perimeter is established during GDA, a distance of 500m to the site boundary is assumed. This is in alignment with RP's safety case assumptions.
- ARF, RFs and DF are set to unity unless their usage is demonstrably pessimistic.
- A ground level release is assumed.
- Conservative assumptions are made for wind speed and weather category at the time of release.
- Inventory is assumed to be at its most onerous accumulation during the plant lifecycle.
- For releases due to an energetic dispersion of radioactive material, such as direct application of an explosive device to the inventory, inhalation dose has been assumed to be the dominant dose pathway.

77. I am satisfied that the above approach represents a robust methodology for the screening out of the low-risk inventory and the identification of higher risk inventory. In determining the potential radiological dose consequences at the site boundary, the RP has adopted a verified and validated ground level inhalation dose formula which accords with UK RGP (Ref. 4).

78. The submission provides evidence in the form of examples which demonstrate how the formula has been applied to calculate dose consequences from the nuclear inventory being sabotaged in specific areas of the plant. Having assessed the evidence, I am satisfied that it produces accurate results.

79. Following the above screening process, the remaining inventory with the potential to give an off-site dose to a member of the public above the lower URC threshold, is subject to further malicious attack-based analysis in Phase 4. This phase applies the UK DBT threats and considers the final damaged state of the plant, sabotage methods and dispersion mechanisms.

Phase 2: Identification of potential Sabotage Event Combinations or potential targets and location analysis.

80. The RP's VAI&C Phase 2 analysis is contained within Annex C (identification of Sabotage Event Combinations (SECs) and potential targets) and Annex D (Location Analysis).

81. The RP's intent within Annex C (Ref. 30) is to determine whether the inventory identified within Phase 1 is capable of leading to a URC following an act of sabotage. This includes both direct sabotage and combinations of acts which could cause the loss of a fundamental nuclear safety function that is keeping the NM/ORM in a safe state. Annex C presents the evidence to support the following argument:

- SECs (comprising Initiating Events of Malicious Origin (IEMO) and SSCs whose sabotage could lead to a URC) have been developed.

82. This annex determines the SSCs that must be protected in order to keep the NM or ORM, identified in Phase 1, in a safe and secure state. First, a set of IEMOs are identified. These equate to events which could compromise fundamental safety functions and therefore have the potential to create a URC. This analysis is carried out for all reactor operating states and fuel movements. The key fundamental safety functions which have been considered are:

- The control of reactivity.
- The removal of heat.
- The containment, shielding, control and limitation of planned and accidental radioactive releases.

83. Aspects of the plant which may be sabotaged, in order to create a URC, are identified at this stage as ‘potential targets’. Where multiple targets need to be sabotaged in order to bring about a URC, these are identified as ‘potential’ SECs. The term ‘potential’ is applied during this phase as the capability of the UK DBT to compromise a target will not be determined until Phase 4 of the methodology. In summary, the key outcomes of this phase are the identification of:

- IEMO
- Potential Targets
- Potential SEC

84. The IEMO, potential targets and potential SECs have been identified through:

- Beyond design basis safety analysis
- Human Factors assessments
- Internal and External Hazards Assessments
- Specialist assessments (e.g. criticality or Probabilistic Safety Analysis (PSA))
- Security workshops

85. I have sampled the above sources of information throughout my assessment, and I consider it to be comprehensive and sufficiently broad to capture the full range of potential sabotage events which need to be mitigated along with the potential targets requiring protection. The RP’s process, and its adoption, meets my expectations and, although additional events and targets will present themselves as the UK HPR1000 design evolves, the methodology applied is repeatable and capable of generating reliable results if consistently applied.

86. The application of this phase of the methodology has generated a table containing a comprehensive list of IEMO and potential SECs for input into the threat assessment (in Phase 3) and the identification of credible IEMO and SECs (in Phase 4). I judge the information presented within the tables to reflect the DR2.2 design and to be sufficiently detailed to enable an adequate VAI&C assessment to be conducted. The UK DBT is subsequently interpreted and applied in the next phase of the methodology.

87. The location of plant, equipment, NM or ORM for each of the potential SECs and potential targets identified in the first part of Phase 2 (Annex C) is set out in Annex D (Ref. 31). This analysis supports the Phase 4 threat assessment and provides the basis for the identification of VAs for protection against sabotage. Annex D presents the RP’s supporting evidence for the following argument:

- Location data for the UK HPR1000 NM/ORM and SSCs has been obtained.

88. Location analysis forms a key component of any VAI study and supports the following aspects of the RP’s assessment process:

- Identification of the physical location of plant, NM/ORM or equipment requiring protection against sabotage.
- Threat assessment and the feasibility study for potential sabotage and attack routes.
- Identification of potential vulnerabilities from a security perspective of the plant design (for example, co-located systems).
- Defining the security architecture and infrastructure.
- Identification of locations requiring protection against theft.

89. The RP's location data has been obtained from the following sources which I consider to be sufficiently broad and detailed to meet the objective of this phase of the VAI&C process:

- 3D Plant Model: this detailed model has been used to identify all rooms which contain key components of each potential target.
- DR2.2 plot plans have been used to identify NM/ORM locations in addition to supplementing the available 3D model data.
- Design and safety case information in the form of the PCSR and supporting design and safety analysis available at DR2.2.
- Design modifications included within DR2.2.
- Plant layout drawings.

90. Having sampled the evidence presented within this annex, I am satisfied that the RP has provided the locations of the potential targets identified in Phase 2 of the methodology. The annex is comprehensive thereby providing a significant amount of detail. I am satisfied that the location data forms an adequate input into the threat assessment, the identification of VAs and that it is based on the latest available information at DR2.2.

Phase 3 and 4: Threat Interpretation and identification of credible IEMO and SECs.

91. Phase 3 and 4 is supported by Annex E and presents the supporting evidence for the following arguments:

Phase 3:
- Relevant documentation has been used to inform the threat interpretation.
- A suitable and bounding UK HPR1000 specific DBT has been developed for application to the assessment of the UK HPR1000.

Phase 4:
- The VAs have been confirmed through application of the DBT to identify those SECs which are within the capability of the applied threat.
- VAs have been categorised based on the magnitude of the potential URC.

92. Annex E (Ref. 32) presents the RP's interpretation and application of the UK DBT (Ref. 10) to the potential targets and SECs identified in Phase 2. Phase 3 of the methodology sets out the RP's interpretation of the UK DBT and Phase 4 applies this interpreted threat to the outputs of Phase 2. This is to confirm or discount potential SECs (both direct and indirect) based on the capability and capacity of the interpreted threat to give rise to a URC through sabotage. In addition, the threat is also used to determine whether NM/ORM can be stolen from the plant in an act of theft. The evidence to support this is presented in Annex F which is directly linked to Annex E.

93. During the early stages of Step 4, at DR 2.1, the RP submitted revision 0 of Annex E. I assessed this submission and identified several potential concerns. These were shared with the RP. In summary, I observed that certain UK DBT threats had been discounted from the VAI analysis without sufficient justification. The RP responded to acknowledge the applicability of the threats, and combinations thereof, and confirmed that it would update Annex E to include them in its VAI analysis against DR2.2, updating Annex E (Ref. 32). My assessment of this submission confirms that the RP has updated the annex in line with my expectations and has consistently applied this revised threat interpretation to its DR2.2 VAI&C submission. I consider the RP's extant interpretation of the UK DBT to adequately support its threat planning assumptions underpinning malicious actor capabilities that need to be considered in its VAI analysis.

94. It should be noted that a number of UK DBT threats remain discounted with the justification for this being provided within the revised annex using claims and arguments. I am satisfied with these exclusions and consider them to be adequately justified for GDA on the basis that the scope is limited to the nuclear island which comprises a large and robust containment structure which is inherently resilient to certain UK DBT challenges. However, during the site-specific phase, the scope of VAI analysis will expand to include the detailed design along with facilities located outside the nuclear island. It is normal practice during the site-specific stage for further VAI&C assessments to take place and for any UK DBT threat interpretation document to be developed for that purpose.

95. Overall, I am satisfied with the RP's interpretation of the threat in the context of the UK HPR1000 GDA for DR2.2. I acknowledge that the RP's case is limited to the available concept design information and therefore will require subsequent review and update by the licensee throughout the site-specific phase.

96. Annex F (Ref. 33) presents the RP's evidence to support the following arguments:

- The NM/ORM inventory has been categorised for theft purposes using appropriate criteria.
- Additional locations requiring protection for the purpose of protection against cyber-attack or theft of NM/ORM have been identified.

97. This annex presents the supporting evidence for the categorisation of the nuclear inventory for theft. The evidence presented in this annex is based on the nuclear inventory presented in Annex A. This inventory is assessed by the RP to identify the appropriate categorisation for theft in accordance with Table 1 of the annex to the SyAPs (Ref. 2). The RP then identifies those locations within the plant potentially requiring further protection against theft of the nuclear inventory.

98. I consider the evidence presented within this submission sufficient to demonstrate that the RP has accurately interpreted the categorisation for theft tables in the annex to the SyAPs. As the tables are stated in the SyAPs, I have not carried out a detailed assessment of all evidence presented on the basis that the inventory data will become more refined during the site-specific phase. I have, however, sampled several of the documents and their conclusions. Consequently, I am satisfied that the categorisation for theft tables have been correctly interpreted. This demonstration meets my expectations for GDA, the analysis will, however, need to be repeated as additional inventory information is generated throughout the site-specific phase. I consider this to be normal business for a licensee.

Phase 4: Identification of Credible SECs and Credible Targets.

99. Phase 4 applies the threat interpretation developed in Phase 3 to the 'potential' SECs to identify those SECs which are 'credible'. It further identifies the SSCs requiring protection from sabotage. It comprises of the following steps:

- The capability required to prosecute each potential SEC from Phase 2 is assessed relative to the DBT capability derived in Phase 3 with the aim of:
  - Identifying those potential SECs that can be credibly prosecuted by the DBT's capability and hence require protection from sabotage.
  - Eliminating potential SECs from the VAI study that cannot be credibly prosecuted by the DBT capability.
- A review of the credible SECs is carried out to judge whether a design solution is able to eliminate the potential for the threat to lead to a URC.

- A consolidated list of targets associated with each credible SEC is developed and their locations are identified.
- Each identified target is reviewed and classified as:
  - A direct target if the target can lead directly to a URC if sabotaged.
  - An indirect target if the target can only lead to a URC if sabotaged as part of an SEC containing multiple targets.
- A structured process is followed to compare the potential SECs derived during Phase 2 with the DBT interpreted in Phase 3. This process considers the following aspects of each potential SEC:
  - Accessibility.
  - Likely sabotage scenarios associated with the potential SEC (in terms of locations and sabotage acts).
  - Likely routes used by an attack group for the identified scenarios.
  - Credibility of the above compared to the interpreted threat.

100. Subsequently, the RP undertook a simple Adversarial Pathway Assessment (APA) to determine the most efficient routes the adversary(s) might take in order to commit the sabotage scenario.

101. Finally, the capability of the threat, drawn from the output of Phase 3 of the methodology is used by the RP to confirm whether the adversary can reach the locations needed in the sabotage scenario and has the capability to commit all of the acts required to cause a URC.

102. The potential SECs are assessed to be ‘credible’ or ‘not credible’ depending on the threat adversary capability to reach all locations required to cause the IEMO and compromise all potential targets within the potential SEC. If the outcome is deemed ‘credible’ then the potential SEC is recognised as an SEC and, the potential targets within it, are designated as targets. If it is ‘not credible’, this is recorded within the documentation for audit purposes.

103. The threat assessment then identifies further potential vulnerabilities which could include locations containing multiple targets, a single location from which multiple sabotage scenarios can be executed or a common point on access routes to several targets. I consider these aspects of the VAI analysis to be an important security input to inform the iterative design process thus enabling vulnerabilities to be identified early and potentially designed-out in accordance with KSyPP1.

104. Following threat application, a list of bounding Sabotage End States (SES) has been generated. Each SES describes the bounding damaged state of the plant following successful prosecution of a credible plant sabotage attack and is subsequently used to support radiological consequence assessments for categorisation purposes. Each credible IEMO (and SEC) has been assigned to at least one SES.

105. Once all IEMOs are assigned to an appropriate SES, a bounding damage state has been defined by the RP. This includes:

- The inventory involved in the sabotage scenario (assuming the most onerous accumulation during the operating lifetime).
- Form of the inventory.
- Dominant dose pathway.
- Bounding sabotage scenarios informed by application of the threat in Phase 4.
- Containment/confinement state.

106. I consider the SES identified by the RP for the UK HPR1000 in Ref. 33 to have been defined in sufficient detail to enable appropriate parameters for the subsequent radiological dose calculations to be undertaken in Phase 5.

Phase 5: Identification and Categorisation of VAs

107. Phase 5 is supported by Annex G (Ref. 34) and presents the RP's supporting evidence for the following arguments:

- The location and categorisation of VAs have been established and plotted on floor plans.
- VAs have been categorised based on the magnitude of the potential URC.
- VAs have been distinguished depending on whether their sabotage can lead directly to a URC or only in combination with the sabotage of other VAs.
- Potential design modifications have been identified during the security assessment of the UK HPR1000.
- The 'secure by design' concept has been applied when considering potential plant modifications identified by the security assessment.

108. The radiological consequences of a release have been undertaken by the RP in Phase 5 of the VAI methodology. This phase considers the final damaged state of the plant following the sabotage attack and calculates the resulting dose consequence at the site boundary. It then compares the dose consequence values against the URC thresholds and categorises the SSCs and locations of the plant as either Baseline, a VA or HCVA. I consider this an adequate approach to substantiate the selection of VAs.

109. The evidence presented in this submission consists of detailed plot plans of each room and SSC contained within the nuclear island requiring protection from sabotage. The RP then applies the graded approach and identifies the required security outcomes for the VAs. I consider this an appropriate way to inform SyAPs 'outcomes' meeting expectations for GDA. The evidence presented by the RP provides the expected detail explained within this annex. It consists of the following information:

- A consolidated list and location of targets requiring protection from sabotage on a room-by-room basis, and all rooms containing at least one target are identified as VAs. This provides the expected level of detail for GDA.
- Radiological consequence assessments are undertaken for each SES derived in Phase 4. Each target is assigned to the SES with which it is associated, and the radiological consequence of each associated SES is captured.
- Each VA is accurately categorised in accordance with Table 1 of Annex B of SyAPs as either a VA or a HCVA based on the radiological consequence of the associated SES(s). This categorisation has been undertaken as follows:
    - Where the sabotage of targets located within a room could lead to a URC (either alone or in combination with other sabotage events) with an offsite dose greater than the upper limit stated in Table 1 of Annex B of SyAPs, the room is categorised as an HCVA.
    - Rooms that contain targets which, if sabotaged on their own or as part of a SEC, could lead to a URC with an offsite dose between the lower limit and the upper limit stated in Table 1 of Annex B of SyAPs are categorised as VAs.
    - Where a room is associated with SESs which have radiological consequences which lead to differing categorisations, the highest categorisation is applied to the VA.

- The RP has helpfully categorised each VA then captured them in both a tabular format and through shaded plot plans. The RP has also provided a means to inform a licensee in shaping a site-specific security plan. The RP has provided a means for developing a proportionate and graded protection regime against sabotage by highlighting:

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

110. I consider that the RP has identified and categorised VAs in a way that informs a conceptual design in achieving a 'graded approach'. This provides a suitable framework for the licensee to develop and apply to the site.

4.3.4 Assessment Summary

111. I consider the RP methodology to have provided the basis for a VAI&C study which meets my expectations. This required me to make judgements against a number of general features attributed to an adequate VAI submission. Specific details of these general features are set out in the TAG with my judgements against each one as follows:

- **Complete.** In its VAI&C analysis, the RP has assumed a loss of off-site power as this cannot be protected by the licensee. In addition, all plant operating states have been considered. Both the active and passive systems required to maintain plant safety have been subjected to detailed analysis. Furthermore, the threat interpretation meets my expectations and a 'graded approach' has been adopted through the identification of VAs and HCVAs.

- **Clear.** The VAI&C submission identifies the protective security 'outcomes' defined by SyAPs, the malicious capabilities in the UK DBT and the radiological consequences that could result. The submission is clear, logical and understandable and the 'golden thread' is easy to follow. The basis for the assumptions and conclusions is adequately explained and justified. Clarity is also provided through the referencing of supporting information.

- **Accurate.** I consider the submission to accurately reflect the UK HPR1000 design at DR2.2.

- **Objective.** I am satisfied that the arguments presented in the submission support the claims made and are sufficiently underpinned by the evidence available at DR2.2.

- **Appropriate.** The RP has calculated the radiological dose consequence at the site boundary with adequate evidence presented within the annexes supporting Phases 2 and 5 of the submission. However, analytical methods to determine the effects of explosive shock and blast have not been employed. Within GDA, the RP has based its analysis on the assumption that any SSC subjected to a highly energetic event will fail. For the purposes of GDA, I judge this approach to be adequate. However, I consider this to be a minor shortfall in that it is an area for improvement within the security case but would be developed further during the site-specific phase of the project when more information is available so that explosive shock and blast analysis is part of further VAI&C submissions. This is an expected aspect of site-specific design analysis and any refinement of the security case.

- **Integrated.** The RP has developed its VAI&C submission providing clear links to relevant engineering and technical substantiation and analysis. This is

demonstrated through the evidence presented in Phase 2 of the VAI&C methodology as detailed above.

- **Current.** The RP has developed its VAI&C submissions using the latest available design information at the time of writing. Within Step 4, the RP has revised various aspects of its submission as the design of the UK HPR1000 has evolved and additional information made available through each DR.

- **Forward looking.** Within the RP's submission it sets the requirement for VA reviews to be conducted to ensure that their categorisation is reassessed against developments in the UK HPR1000 design, layout, nuclear inventory, safety case or changes to the UK DBT. Again, this is an expected activity as any future change to the design would require an assessment of the consequences of such change for vital areas.

4.3.5 Strengths

112. All five phases of the RP's methodology have been implemented using DR2.2 and safety information which has led to a comprehensive VAI&C study sufficient to inform a conceptual security regime. The approach reflects the expectations within SyAPs that draws from international RGP. Moreover, it provides a licensee with the wherewithal to reassess the design and plant after GDA. The RP has achieved this by:

- The application of RGP, coupled with innovative approach, that has created additional analysis that further informs a 'graded approach'.
- Providing a consolidated list of VAs for the UK HPR1000 which have been suitably categorised.
- Providing a set of plot plans identifying the locations of VAs, including those which are 'direct' and 'indirect'.
- Identifying the locations within the plant potentially requiring additional protection against theft of NM or ORM that have been included on the plot plans.
- Offering a methodology, and its application, so to inform the developing design of the UK HPR1000 in accordance with 'secure by design' principles.

4.3.6 Outcomes

113. Through my assessment I have not identified any AFs, however, I have noted one minor shortfall.

4.3.7 Conclusion

114. The RP has developed a workable VAI&C methodology and has adequately implemented it against the design. The RP has provided a full and detailed document set. The documents meet expectations in terms of drawing effectively from RGP and are SyAPs aligned. I consider that:

- The full range of UK DBT threats have been considered. Where they are screened out from further analysis, sufficient justification is provided.
- In conducting its VAI&C analysis, the RP has considered the threats set out in the UK DBT in combination and in doing so has identified realistic yet worst case threat scenarios.
- The interdependency between SSCs in delivery of safety functional requirements has been considered.
- Both active and passive systems required to maintain plant safety have been considered in the analysis.

- The RP's submissions present a clear linkage between the identified VAs, the relevant malicious capabilities and the radiological consequences that could result from such action thereby informing the conceptual security regime.
- The claims and arguments are well supported by evidence.
- Analytical methods and computer modelling tools for dose consequence determination are sufficiently justified as being fit for the intended purpose.

115. I have carried out a comprehensive assessment of the RP's VAI submissions. I consider the RP to have presented sufficient detail in terms of claims, arguments and evidence to meet regulatory expectations commensurate with SyAPs, RGP and the scope of GDA. There are no AFs and one minor shortfall regarding blast analysis.

4.4 Cyber Security

4.4.1 Assessment Approach

116. For my cyber security assessment, I expected to see how the RP has considered cyber security in its support to both the overall safety and security regimes for the UK HPR1000 design. The safety aspects are managed through the C&I specialism. Whilst complimentary, both safety and security have specific requirements for cyber security. As a key concept for cyber security, I adopted the position that any computerised system can be altered, as by their very nature they are designed to be altered. These alterations can be intentional, both malicious and non-malicious, or accidental. This approach assumes that an unauthorised change will occur, and that the RP has considered both 'secure by design' and 'defence in depth' for the licensee to be able to detect the change, initiate a suitable response and recover control of the systems. I sought evidence that cyber security had been considered within the plant architecture, the protection of individual systems (barriers forming a 'defence in depth' described at KSyPP 4) and the depth of cyber controls (identify, protect, detect, respond and recover) so to meet my expectations based on SyAPs and specifically Cyber Protection Systems (CPS) 'outcomes' within the SyAPs. Therefore, I expected to see the claims, arguments and evidence that the RP makes in respect of the risk assessment, controls and substantiation of those controls to achieve the CPS 'outcomes'.

117. I also expected to assess the strategies for activities needed to support those claims, arguments and evidence, in the form of security production excellence and security assurance. I sought to confirm the UK HPR1000 generic design is resilient to sabotage that causes a URC and assists in the prevention of the theft of NM, rather than being impervious to cyber-attack. The final area that I sought to assess by sampling was that the RP had conducted due diligence in the cyber security of future CBSy systems.

4.4.2 Cyber Security Risk Assessment

118. I reviewed the Cyber Security Risk Assessment (CSRA) methodology (Ref. 19) to further inform my sampling. The steps within the methodology are:

- Step 1 – Determine systems and their security level
- Step 2 – Identify system vulnerabilities
- Step 3 – Application of the cyber elements of the threat interpretation document
- Step 4 – Initial risk assessment
- Step 5 – Cyber protection system outcomes and control sets
- Step 6 – Residual risk assessment and remedial measures
- Step 7 – Claims on combinations

119. The Cyber Security Risk Assessment Report (CSRAR) (Ref. 20) is the result of the application of the CSRA methodology and forms the basis of my sampling. Section 4 of the CSRAR presents more details of how each step of the methodology had been

conducted and then in Section 5 details how those steps reflect on each of the eight identified systems in Step 1. In Step 1 the RP evaluated the systems within scope of the GDA Project (Ref. 7) scope to identify which systems are considered CBSIS and apply a security degree. The RP also analysed those systems for interconnections and dependencies, to which they identified another 6 systems that needed security degrees to be applied. Those systems are:

- Plant Standard Automation System
- Reactor Protection System
- Safety Automation System
- Severe Accident System
- Diverse Actuation System
- Plant Computer Information Control System
- Main Control Room System
- Remote Shutdown Station System
- Nuclear Instrumentation System
- In-core Instrumentation System
- Rod Position Indication and Rod Control System
- Plant Radiation Monitoring System
- Turbine Generator Control System
- Nuclear Accident Emergency Monitoring System

120. I consulted with the lead C&I inspector and reviewed the VAI&C reports, covered in sub-section 4.3 of this report, to confirm the selection of these systems matched ONRs expectations, which they did. The C&I assessment report (Ref. 40) contains more detail on the selection of these systems and the application of their security degree.

121. I sought evidence that the CSRAR had been based on RGP and recognised standards. Security degrees are based on the IEC 62645 (Ref. 12) standard. Step 5 of the RP's methodology identifies the appropriate CPS outcomes expressed in Annex H of SyAPs and is based on an ISO/IEC 27005 risk assessment structure. This step then examines the CPS outcomes, responses and functions against the threat actor's skill level. This analysis informs the control set selection in terms of what controls are needed to satisfactorily address the risks. The control sets have been selected from several international standards. Primarily they are from IEC's 62443-3-3:2013 and 62645:2014 with selected controls from 61513:2013 & 61508:2010, (Ref. 12). I consider this a suitable approach and aligns with RGP.

122. The control sets are identified as:

- A – Access Controls (A1-A4)
- B – Connectivity (B1-B7)
- C – System Development (C1-C3)
- D – System Functionality (D1-D12)
- E – System Monitoring & Audits (E1-E4)
- F – Security Management & Planning (F1-F5)
- G – Testing / Verification / Validation (G1-G3)
- H – Configuration Control and Modification (H1-H3)
- I – Recovery Operations (I1-I2)
- J – Confidentiality of Information (J1)

123. The individual system risk assessments follow the basic framework of ISO/IEC 27005 (Ref. 12) of conducting an unprotected risk assessment, identifying and applying controls and then conducting the risk assessment again with the controls to establish if the risks are within tolerance. Where they are not, a risk management process is applied or it is noted for the licensee to address at the site-specific stage. This approach to conducting a risk assessment matched my expectations.

124. Having identified the controls needed, I sought evidence of how they will be implemented. The controls themselves are detailed in the Cyber Security Design Requirements Specification (CSDRS) (Ref. 41) and then a compliance gap analysis is undertaken for each of the eight identified systems. The compliance analysis enables the RP to establish what is in place, what requires a design modification, what is a design requirement, what requires enabling activities and what is for the future licensee. Most of the controls are evidenced within the System Design Specification (SDS) and System Requirements Specification (SRS). The SDS document specifies the function, performance, architecture and other design features of the systems. The cyber security regime is also captured in the SA/SI and CONOPs documents. However, during GDA the RP assessed the compliance status of two systems that had undergone the cyber security compliance analysis and updates to their SDS and SRS documents. Whilst I consider this to be a shortfall of note, the key architectural items for the remaining six systems are contained within the CSRAR. I therefore have adequate confidence in the broader risk assessment. I therefore consider an AF is needed in order that the compliance analysis is completed for these remaining systems by the licensee at the site-specific stage.

AF-UKHPR1000-0047 – The licensee shall complete cyber security compliance analysis for all computer-based C&I systems important to safety and implement measures to address all instances of partial or non-compliance.

125. As part of my assessment, I have also reviewed the TSC's report (Ref. 42) and consulted with the lead C&I assessor. The RP's CSRA methodology is based upon the RGP contained within ISO/IEC 27005 (Ref. 12) and IS1&2 (Ref. 11). When the CSRA methodology is compared to the National Cyber Security Centre's (NCSC) Cyber Assessment Framework (CAF) (Ref. 11) as another source of RGP, for the principle A2a risk management process, I consider that it meets the achieved criteria as described in the CAF.

126. To bring all of these aspects together, I considered the 'golden thread' from identifying the systems, grading those systems, considering threats, vulnerabilities and calculating the risks. The risks then have controls applied to them and the risk values are recalculated, with risk management controls applied where necessary. In the final stages the controls are confirmed as being in place, whereas at an operational station it would be confirmed that such controls are effective and efficient. I judge this to be in line with most approaches to risk assessment and in particular ISO/IEC 27005 (Ref. 12). The full control set for IEC 62443-3-3 (Ref. 12) has been analysed by the RP with controls only being discounted with justification. These controls are then enhanced by the RP with specific controls selected from other standards based on engineering experience to provide additional targeted controls.

127. I consider the approach used by the RP is appropriate and matches the regulatory expectations contained within TAG 7.1 (Effective Cyber and Information Risk Management) (Ref. 4) and 7.3 (Protection of Nuclear Technology and Operations) (Ref. 4), in that a risk-based assessment has been undertaken with regards to the systems and that the CPS 'outcomes' can be achieved in the UK HPR1000 design. I conclude that the RP has conducted sufficient preparatory work for a licensee to implement the expectations of TAG 7.5 (Preparation for and Response to Cyber Security Incidents) (Ref. 4).

128. The unsophisticated nature of the ISO/IEC 27005 (Ref. 12) risk assessment provides an adequate approach at a system level, but I consider it lacks the details for different components within a system. Within the risk assessment some of the controls changed focus from the main system under consideration to the support tools like the engineering workstation. In one sample I assessed that a particular control, application whitelisting, was not applicable to the system under consideration as the software ran

directly on the hardware and there was no intermediary operating system that could host applications or the application whitelisting. The compliance evidence cited was that the engineering workstations could have application whitelisting post-GDA. Further sampling in this area did not establish any shortfalls that affected the main system under consideration. I consider this matter to be of significance and therefore the licensee should demonstrate this matter has not propagated across other controls. I have raised the following AF.

AF-UKHPR1000-0054 – The licensee shall, as part of detailed site-specific design, demonstrate that the security controls identified in each of the cyber security risk assessments have been considered against the core platform/component delivering the safety/security function. Peripheral components (for example maintenance workstations) must also have suitable security controls selected based on the threat they pose to the core platform/component.

129. I also considered that the risk assessment process had other anomalies and whilst they did not materially affect those items within scope of the GDA, continued use of the process in its current form for an approved nuclear site security plan may prove insufficient. I would expect that if a licensee wishes to adopt these processes within their security plan that they would undertake a review to ensure that it will support their ongoing security needs. I consider this to be a minor shortfall for GDA.

4.4.3 Cyber Security Architecture

130. As well as the risk assessment, I assessed the cyber security architecture. This forms another key element of the claims and controls presented in the CSRAR. The RP submissions list numerous communication interfaces but these are mostly hardwired. When considering cyber security architecture, I applied Health & Safety Executive guidance on Cyber Security for Industrial Automation and Control Systems (Ref. 43), which describes hardwired connections as to typically handle conventional analogue signal types such as 4-20mA loops or discrete voltage levels (0-5v). The RP details several network devices that do not have a device specification, but functional requirements. These can be identified as gateways and Communication Interface Modules (CIM). The gateways have requirements that indicate they are firewalls or data diodes that provide boundary controls to systems within different security domains. As these devices only have requirements, I have judged it a suitable approach to ensure cyber security devices for use in the UK HPR1000 will be selected based on meeting the functional requirements and UK cyber security assurance standards.

131. As well as compliant and hardwired interfaces, I considered the non-compliant interfaces and the interfaces to systems declared outside the scope of the UK HPR1000 GDA Project (Ref. 7), as far as establishing the context of the security on those interfaces. During the GDA process both the C&I assessor and myself were able to influence the non-compliant and out of scope interfaces and have seen a number eliminated through design modifications. However, there still remains a number of commitments to further design modifications that will address the remaining non-compliant interfaces and to assess the out of scope interfaces. These have been referred to by the RP as ‘deferred design modification’ for cyber security. I, along with the C&I assessor, consider these items of significance and that they need to be formally managed through to resolution. For that reason, we have raised the following two AFs. The first is to address the known shortfalls in the cyber security architecture, in the deferred design modifications. The second is to reaffirm the risk assessment remains valid through these and other anticipated modifications and development of the systems.

AF-UKHPR1000-0046 – The licensee shall resolve the residual cyber security vulnerabilities identified in the GDA cyber security risk assessment report as part of detailed design. This should include the potential modifications proposed during GDA.

AF-UKHPR1000-0045 – The licensee shall, as part of detailed design of the C&I systems, develop the cyber security risk assessment to include all C&I systems important to safety, and all interfaces between and within those systems. The assessment should follow a methodology that is at least as rigorous as that developed for GDA, and should include demonstration that measures are in place to address all identified vulnerabilities.

132. The RP also makes a compliance statement against NCSC secure design principles (Ref. 11). I see this as a welcome approach and, whilst the depth of the compliance statements in these submissions are high-level, their inclusion can only benefit the future licensee.

4.4.4 Production Excellence for Cyber Security

133. Another aspect I considered was the production excellence for cyber security. The RP identifies a number of standards it will apply in order to deliver production excellence for the UK HPR1000. These include ISO9001, IEC 61508, IEC 61513 and IEC 60880 for higher class safety systems. The RP's submission recognises that these are for the safety demonstration of production excellence and may not fulfil the purpose for security. To support the demonstration of production excellence for cyber security, the RP makes a compliance statement against the NCSC Commercial Product Assurance (CPA) build standards (Ref. 11) thirteen requirements. The RP then analyses this compliance and identifies actions for the licensee to undertake. However, weaknesses in the wider production excellence area have been identified by the C&I assessor. These weaknesses, that include cyber security as one of the twenty-one areas identified by the RP, were followed up in RO-UKHPR1000-0059 (Ref. 37) and are considered further within the C&I assessment report. Taking into consideration all of these points from a security perspective, I was satisfied with the RP's strategy to deliver production excellence for cyber security.

4.4.5 Cyber Security Assurance

134. During GDA I influenced the RP to explain their strategy for conducting cyber security assurance. The detailed implementation of which will be for the licensee at the site-specific stage. Whilst there are no standards on how to conduct this activity within the context of a nuclear power station control system, similarities can be drawn from IEC/ISO 15408:2009 (Ref. 12) Information technology - Security techniques - Evaluation criteria for IT Security and from the NCSC's CPA process for performing evaluations at foundation grade (Ref. 11). Within these standards, security products (firewalls, encryption, and trusted platform modules) are evaluated for their soundness to perform their intended purpose. As part of the evaluation a number of other activities are conducted on the target devices to identify vulnerabilities.

135. Within the CSRAR (Ref. 20) the RP identifies that independent assurance activities will be conducted. Also, within Control Set G, 'Testing / Verification / Validation', there is information on security assurance based on IEC 61513 (Ref. 12) and the testing identified within the quality production plan required within the IEC. For GDA assessment purposes both the C&I assessor and I considered this insufficient to understand the strategy for security assurance. Following RQ-UKHPR1000-1707 (Ref. 44), the RP provided a new appendix for the CSRAR in the RQ response. The appendix presents a methodology called Independent Security Assurance Measures (ISAM) and is linked to Independent Confidence Building Measures (ICBM), drawing

out a need to coordinate the two strategies. I, along with the C&I assessor, found the ISAM strategy to be more than satisfactory and having great potential to advance RGP in this area. I am content that a licensee will be well placed to take this forward.

4.4.6 Computer Based Security System

136. Outside of the plant systems there is a regulatory expectation that the RP will explain the approach to cyber security of the CBSy. For cyber security of the CBSy, I was not looking at the function of the system, but the confidentiality, integrity and availability aspects of a future system. Within the CSRAR, SA/SI and CONOPs (Refs. 20, 21 and 22) it is identified that the main components of a future security system, and hence its CBSy, will be located outside of the nuclear island. Therefore, the final CBSy solution will be a matter for the licensee. However, I needed to be content that the RP had conducted due diligence that an adequate security system can be installed in the UK HPR1000 generic design. I sought evidence that the RP had considered if there is the appropriate room, power, back-up power and is appropriately secure. The approach detailed by the RP I judged appropriate for the licensee to implement. It is also the approach used in the reference plant FCG Unit 3. Analysis by the RP indicate power, cable runs and network infrastructure will be minimal within the nuclear island.

137. As well as looking for due diligence by the RP, I was looking for indicators of RGP being captured in the strategy to deliver cyber security for the CBSy. The Centre for the Protection of National Infrastructure (CPNI) Cyber Assurance of Physical Security Systems (CAPSS) is recognised as providing RGP and product assurance for CBSy equipment. Whilst the RP does not cite CAPSS, both the RP and CAPSS identify the NCSC CAF 3.0 (Ref. 11) as an assessment tool to sit alongside the CSRA methodology for the strategy to deliver a cyber secure CBSy. I consider this a suitable approach which meets expectations. The delivery of a secure CBSy system is a different aspect to the functionality of the CBSy and its integration into other security components to deliver the PPS outcomes. This is considered later in this report.

4.4.7 Strengths

138. I judge that the RP has adopted a suitable framework to demonstrate that CPS outcomes are achieved. Within that framework, multiple standards and RGP have been followed to calculate the cyber security risk, to identify the controls needed to address those risks and to finally demonstrate the residual risk levels. In selecting the controls, the RP has not limited themselves to the controls within GDA scope. They have presented their vision of how they see the licensee implementing controls beyond the scope of GDA in order to present the complete picture for cyber security.

139. The RP has taken RGP for cyber security assurance from the cyber security products sector (e.g. vendors of firewalls and Virtual Private Network (VPN) devices) and developed a strategy to deliver ISAM that fits the needs of the nuclear sector. Not only have they developed this as RGP for the nuclear sector, but they have identified the need and developed a strategy to integrate this with the safety requirement to demonstrate ICBM. This is the highpoint of developments made by the RP for cyber security.

140. For CBSy, the RP has adopted an approach already under construction at the reference plant. Whilst the detail of the cyber security aspects of CBSy are outside the scope of GDA, the strategy put forward provides confidence that both the resourcing (e.g. cabinets and power) and the cyber protection of the CBSy, using the CSRAR and CPNI guidance, are achievable.

4.4.8 Outcomes

141. Based on my assessment of cyber security there are several matters that have not been addressed within the GDA timescale. The key items are the AFs detailed above and summarised as:

- To apply the compliance gap analysis to the other CBSIS within scope of GDA.
- To improve evidence regarding some of the controls within the control sets.
- To conduct the modification process on the identified system interfaces.
- To conduct further cyber security risk assessments as information becomes available for the out of GDA scope interfaced systems.

142. Whilst the AFs are worthy of being tracked to completion, the shortfalls identified fall on the periphery of the systems sampled. The underpinning items, like cyber security architecture, were much stronger and support the position that these matters can be resolved in the site-specific stage by a licensee. There were other minor shortfalls also identified and these are noted in the assessment above and captured in my cyber security assessment note (Ref. 45). Again, these shortfalls do not undermine the security case in GDA, but they could prove problematic for a licensee unless considered at an early stage.

4.4.9 Conclusion

143. Based on the outcome of my assessment of cyber security for the UK HPR1000, I have concluded that I have sufficient confidence that a licensee can implement adequate arrangements to protect CBSIS based on the development of the risk assessments and the modifications/commitments identified. I have also concluded that there is a sufficient strategy to deliver cyber security assurance and there is an appropriate security architecture. This meets the regulatory expectations for cyber security as laid out in SyAPs, primarily under FSyP 7 (CS&IA), and the associated TAGs. The RP has provided sufficient evidence that the CPS outcomes can be met in the UK HPR1000 generic design.

144. The strategy to deliver production excellence for cyber security feeds into the wider production excellence area. The weaknesses identified by the C&I assessor do not materially affect the strategy that I have assessed. It would, however, degrade the implementation of the strategy. I have concluded that there is a sufficient strategy in place to deliver production excellence for cyber security, where it is supported by an adequate wider production excellence process.

145. I have also concluded that there is sufficient due diligence by the RP that a licensee can install a foreseeable CBSy system that could meet the required CPS outcomes.

146. In my assessment of cyber security, I have identified four AFs, three of which have aligned with and are also stated in the C&I assessors report. These AFs are AF-UKHPR1000-0045, AF-UKHPR1000-0046, AF-UKHPR1000-0047 and AF-UKHPR1000-0054. These are detailed above and collated in Annex 2 of this report.

4.5 Conceptual Security Regime

4.5.1 Assessment Approach

147. The expectation within GDA is that the conceptual security regime completes the ‘golden thread’ from analysis to a generic solution. That is, a solution should provide a SyAPs aligned security conceptual framework from which the licensee would seek to develop its more detailed security plan at the site-specific stage of development. I also sought evidence of the RP taking a more holistic view, based on SyAPs, that examines both cyber and physical risks and then explains how the design is protected.

148. The relevant submissions that describe the RP's conceptual security regime are the SA/SI (Ref. 21) and CONOPs (Ref. 22) documents. This part of the RP's submission is the output from their risk assessments for judging the cyber and physical risks to the design. These risks are related to both sabotage and theft. However, much of the security architecture and infrastructure, together with the way it operates, is a licensee's decision. Nevertheless, I expected to see how the RP sought to differentiate between what is realistic in GDA and what might be a licensee's choice. Therefore, in making this distinction, the RP is expected to provide the licensee with a suitable framework from which to develop a security case and thereafter a security plan. So, taking account of the limitations within GDA as they relate to a security regime, I sought evidence that these documents provided a suitable framework, based on security functions, which the licensee could develop into more detailed requirements for protection systems.

149. Given the specific technical expertise required to deliver this aspect of the security case, I sought confidence that the RP had drawn on the expertise within the supply chain. Moreover, that the RP had acquired the necessary capability to deliver the level and quality of detail for a meaningful security risk analysis and case.

150. Reflecting the assessment plan for Step 4 (Ref. 5), I have used elements of SyAPs to inform my judgements. Most relevant are the KSyPPs. These principles are the most germane to GDA, therefore I sought evidence that these have been foremost in the RP's analysis and explanation of a conceptual security regime. Also, within my Step 4 assessment plan (Ref. 5), I highlighted both FSyP 6 (PPS) and 7 (CS&IA) as relevant. Specifically, I assessed the RP's conceptual PPS design framework against SyDP 6.3 (PPS). I also assessed their framework for resilience against cyber threats described at SyDP 7.3 (Protection of Nuclear Technology and Operations).

151. SyAPs, as the principle regulatory guide to making my judgements, is informed by an international framework of guidance that includes the responsibilities of the State that are relevant to GDA. I mention these references for completeness and wider context to my assessment. Specifically, the Convention on the Physical Protection of Nuclear Material (CPPNM) (Ref. 9). Further explanation of international commitments is in NSS 13: Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5) (Ref. 9), which provides guidance on the physical protection of NM and nuclear facilities.

152. I have drawn from experience and the advice from the CPNI in making my assessment. CPNI is the UK government authority for protective security advice to the UK national infrastructure. I have also drawn on guides produced by the World Institute for Nuclear Security (WINS) and specifically on 'secure by design' (Ref. 46).

153. Specific to GDA is the Security GDA TAG (Ref. 4) that provides guidance on assessing the RP's submissions and has informed my judgements.

154. All these reference documents were discussed with the RP over the various steps of GDA. Their application of RGP, through developing their GSR, was 'enabled' through routine and periodic meetings and workshops. Specific meetings were held to cover the interaction between cyber security and C&I systems given the clear synergy.

155. Through such an enabling approach, the RP developed its Tier 2 submissions throughout both Steps 3 and 4. Building on assessments in previous steps, and the RP's maturing security case, I assessed the DR 2.2 SA/SI (Ref. 21) and CONOPs (Ref. 22) documents against the assessment plan for Step 4 (Ref. 5). In taking a sampling approach, I focused my assessment on the subject areas covered in the following paragraphs.

4.5.2 Comparison to Key Security Plan Principles

156. In terms of RGP, and this GDA, I consider that the RP has drawn sufficiently from suitable sources and specifically CPNI for adversary capability and consideration of doors, identifying appropriate performance levels. Particularly, they have explained in detail the application of CPNI's Manual Forced Entry Standard (MFES) (Ref. 47), its adversary capability and Loss Prevention Standard 1175 for assessing the delay function. Protection against theft is integrated into their analysis in a workable manner. While they might have broadened the sources of RGP, they have referred to some learning from previous GDAs. For GDA, this is acceptable as my expectation was for the RP to list security capabilities, such as CCTV, purely as an illustration of what might be selected by the licensee.

157. I sought evidence that the RP had explained their approach to achieving 'secure by design' (KSyPP 1). Throughout my interactions during Steps 3 and 4, I emphasised the need to first explain, then apply, a 'secure by design' approach. The RP has used its CONOPs document to provide a comprehensive description of 'secure by design'. This includes adequate reference to their risk analysis. I judge that it has been developed in a logical manner starting with their priorities for protection based on the level of risk. They have refined their risk assessment by adopting a matrix that is based on wider security industry RGP. For GDA, I judge that the RP has an appropriate understanding of 'secure by design'. They have provided suitable evidence of being actively engaged within the wider modification process that includes post-GDA commitments. Within the CONOPs, the design modifications, as they affect security or arguably reduce security risk, are captured and explained in adequate detail. They have provided evidence of working with designers and engagement within the wider modifications process. I judge that they understand the design itself and the potential to manage risk through modifications. For this GDA, I consider that the RP's methodology for delivering 'secure by design', and its application, meets expectations.

158. Related to 'secure by design', I sought evidence that the RP had deconflicted security conceptual design with safety measures and especially evacuation routes in high-risk areas. This is a practical consideration within the scope of GDA. I consider that the RP has addressed this aspect satisfactorily, and a modification has been identified that provides evidence that this topic has been captured formally.

159. Considering KSyPP 2 (the threat), the RP has provided a broad and useable description of the DBT within their Threat Interpretation document (Ref. 15). I also found their examination of the adversary helpful in terms of drawing from CPNI RGP. For example, in applying the MFES and against a 'knowledgeable' attack force. They also describe, with adequate analysis, the bounding adversary pathways through an appropriate examination of staircases and doors leading to room access. I therefore judge that they have conducted sufficient analysis to apportion additional protection to selected areas and routes as they seek to potentially degrade any adversary's freedom of movement towards targets for theft and sabotage. This is RGP and has been applied in detail.

160. I sought evidence that the RP had developed a way of explaining their method to achieving a 'graded approach' (KSyPP 3) that provides the basis for ensuring risks are proportionally addressed within a conceptual security regime. The RP has rightly focused much of its GDA resource to the analysis of the risks inherent in the design. This has demanded a detailed and comprehensive examination of the nuclear inventory and security related safety systems, drawing from the safety case, to identify and categorise VAs and conduct a similar risk analysis of the cyber threat using the UK DBT and other credible sources of information. I found that their SA/SI methodology takes the output of this risk analysis work and develops it further by explaining the variations of VAs. That is, drawing from their VAI&C assessment, how they have differentiated between direct and indirect targets that would affect an adversary's

actions. They have conducted a similar approach for the Categorisation for Theft (SyDP 6.1). For GDA, this is a satisfactory way to provide a framework to address KSyPP 3. I therefore judge that the analysis provided by the RP to underpin a 'graded approach' meets my expectations.

161. I expected the RP to explain how, within the limitations of GDA, the SyAPs 'outcomes' and related indicative 'postures' would be achieved through security functions. These functions of 'detect', 'delay', 'assess', 'respond' and 'access control' are used in KSyPP 4 as ways to describe 'defence in depth'.

162. In creating 'defence in depth' (KSyPP 4), the RP has responded by categorising different layers such as the building exterior shell and then VAs. Therefore, I am satisfied that by allocating security functions to each layer, and then having multiple independent barriers at building and room boundaries, they have described how the necessary depth is achieved, thereby meeting my expectations. They then add further detail by offering elements of a generic security capability. For example, they examine security doors, CCTV, and Automatic Access Control Systems (AACSs). They then map these back to the SyAPs 'outcomes' and 'postures' through examination of security functions. Using RGP, and in a complex but necessary framework, the RP has effectively linked security areas to systems that include generic capabilities that deliver such security functions. While at times this seems intricate, I judge it to be a logical means by which to describe the priorities within a conceptual design. I consider the RP's framework, that addresses KSyPPs 3 and 4, as a suitable means to assist the licensee when allocating security to given locations as being proportionate to the risk and one that is sufficiently evidenced. While the RP's framework to explain how depth might be achieved makes sense, it tends to focus on a Physical Protection System (PPS). The RP carries out a similar exercise for CPS using security degrees and control sets as part of a recognised lexicon of RGP terms. Overall, and within the context of GDA, I consider that the RP has covered this principle in adequate detail and provided a workable framework on which the licensee could then apply proportionate and targeted security arrangements.

163. For KSyPP 5, (Security Functional Categorisation and Classification), I sought to see how the RP had addressed this within the context of GDA. The application of security categorisation and classification is a relatively new security regulatory and civil nuclear security concept and RGP is developing. However, I am satisfied that the RP has a scheme to strengthen areas of greater security risk in a proportionate manner using some of the terms and methods from RGP.

164. I also found the way the RP has developed the tables that capture most of the KSyPPs as helpful to a future licensee. For example, they provide tables in which they capture the concepts of 'categorisation and classification' against outcomes, offering illustrative security capabilities against security functions that are then allocated various priorities for protection. I consider that these tables and frameworks will inform the licensee and be of value in making a security case for the site-specific stage.

165. Considering KSyPP 6 (Codes and Standards), these have been used and referenced within the SA/SI document. I am satisfied that the various industry standards have been sufficiently examined providing a signpost for the licensee. The RP has used standards albeit noting that the licensee will develop systems and equipment through their requirements management. For example, they refer to PAS 68 (Ref. 48) when explaining Hostile Vehicle Mitigation (HVM) as part of a list that covers both physical and cyber ISOs, British Standards and other relevant industry standards drawn from recognised RGP. The RP explains, in some detail, the MFES (Ref. 47) test ratings as they relate to doors, hatches and vents offering some performance classifications.

4.5.3 De-conflicting Security design with Safety functions and Measures

166. In RQ-UKHPR1000-0706 I sought assurance that in achieving the requisite security measures, these activities do not unintentionally degrade critical safety functions and related procedures. As a topic this was deemed an area of consideration within GDA, although more relevant in detailed design. Within the context of GDA, I asked the RP to explain how they had worked with other specialists and the designers to identify where and when potential security functions could affect safety measures. While seeking adequate evidence that this topic was considered within GDA, it was agreed that a full human factors assessment of security systems would only be possible and realistic once the licensee had developed these after GDA.

167. The RP responded by explaining that they had actively shared their security case with design engineers. Specifically, they had provided the locations of the safety SSCs that must be protected to prevent the sabotage of NM/ORM that could cause a URC. The CSRAR (Ref. 20) also identified several security risks to centralised C&I systems that deliver safety functions and highlighted the necessary protective measures.

168. The RP referenced the emergency evacuation routes from the relevant reports. They explained that door schedules, that included safety features, had been designed so to deconflict with any security measures. The RP also explained that they had produced a modification design meeting schedule so to build mutual understanding between safety and security staffs. In a similar vein they had held workshops to educate the relevant core staff on their security risk assessments and outcomes, and how they had interacted with safety and environmental teams.

169. There was evidence that the RP security team had been consulted on the various design modifications associated with the UK HPR1000 through the GDA design modification process. As the conceptual design of the security functions and measures was developed, they discussed these measures with subject matter experts within a programme of workshops.

170. The RP explained that given most of the security regime would be developed by the licensee, only a limited number of incidents of potential conflict between safety and security requirements were identified during GDA. However, within their documents they have explained the process by which the security regime will be considered alongside the requirements from the safety case.

171. I examined the RP's response to this topic that they captured within their DR 2.2 documents. The RP has covered this subject adequately for GDA noting that this is an area the licensee will need to consider when developing more detailed security capabilities. The RP therefore has met my expectations.

4.5.4 Electrical Power to Security Systems

172. In RQ-UKHPR1000-0694 I sought an understanding of the security demands on the electrical power system. Because this topic appeared as an AF in a previous GDA, I selected it as an area to sample. In their concept of security, the RP explained that their security infrastructure would be located both inside and outside the nuclear island. Infrastructure outside the island, and not within GDA scope, could include facilities and capabilities such as a gatehouse, Security Control Room (SCR) or Security Operations Centre (SOC), fences with CCTV and security lighting amongst other capabilities. While developed later in the site-specific stage, I expected them to be acknowledged within the GDA security case. But specifically, for the plant in-scope, security systems, albeit conceptual in nature, will require robust and resilient power supplies when developed further. I therefore asked the RP to confirm how such security systems, and those in-scope for GDA, would acquire their electrical power.

173. The RP stated that initial power will be supplied to the components of the security regime from the grid. Standby power will be provided from an emergency generator, until grid power can be restored. A finite period will be required to bring the emergency generators online. Therefore, an Uninterruptable Power Supply (UPS) will be required to bridge this gap. The current GDA design for the UK HPR1000 includes three emergency diesel generators and two station blackout diesel generators to provide emergency power to the Class 1 safety systems. To preserve any spare capacity within these generators, and to provide some redundancy to the security components, the RP proposed that emergency power for the security solution would be provided through two dedicated emergency security diesel generators. These generators could be located within the main and alternative security gatehouses that will be considered in the site-specific design phase of this project. This potential solution is also recognised as RGP.

174. The RP stated that power requirements for the integrated security solution for the site-specific design of the nuclear power station will not be known until the licensee has completed its detailed design. I am content with this approach for GDA but note that the licensee would be expected to assess the power requirements for their whole site security arrangements and the locations for the security emergency diesel generators, UPS and power distribution networks as a priority.

175. With an expectation that a licensee would consider this topic as integral to their development of a whole site integrated security solution, I was content that the requirement was sufficiently understood by the RP and is included in their submissions for GDA.

4.5.5 Assessment Summary

176. Overall, I have identified one matter that I consider as an AF that should be addressed early in the site-specific phase. It is for the licensee to take and develop the GSR into a security plan. During GDA, the RP has offered a framework to deliver a conceptual security regime that is aligned with SyAPs. While that framework categorises locations for certain levels of protection, it does not specify the details of systems. It is for the licensee to provide the requirements for specific systems that deliver security functions such as ‘detect’. Allocating sufficient space for such anticipated security infrastructure, drawing from operational experience, needs to be examined early after GDA. This site-specific activity needs to be tracked by ONR as the information necessary to resolve this matter is not readily available during GDA. I therefore identified this AF:

AF-UKHPR1000-0055 – The licensee shall, as part of site-specific detailed design, identify the facilities, equipment and support necessary for the security system. It should be a priority to secure sufficient space and support for the security equipment and activities, and to integrate and deconflict it with other plant systems, so to deliver the security outcomes sought as part of the site-specific security case.

177. Additional to this AF, I also identified these minor shortfalls. These areas for potential improvement are explained below.

178. The RP examined the risks based on the Main Control Room (MCR) and Remote Shutdown Station (RSS). Given their significance in plant operations these security risks and mitigation could be examined and developed further to improve the security case. This would be expected as normal business for the licensee when taking the security concept into detailed design.

179. The RP examined the use of lifts between floors as an adversary pathway. While I am content with their examination of this topic, it will be for a licensee to consider access

control when making choices regarding security systems such as access management and CCTV and their locations.

180. The RP describes the SOC/ASOC as managing both physical and cyber security as two functions in one location. While this is a potential innovation in monitoring security systems, the case will need to be developed further after GDA to identify and assess the benefits and drawbacks of such integration of these functions.

181. The RP has given illustrations, or strategic intent, of security capabilities for example CCTV and AACS identifying some standards and broad requirements. While this sets the conditions for a licensee in making detailed decisions on types of security systems and locations, the RP has not examined in any detail the challenges of system integration given the complexity involved. This includes the likely demands for a network and related cabling for security systems. Also, the space for these systems and their environmental support. By addressing the challenges of security system integration early in the site-specific phase, the licensee will be able to improve the security case.

182. The RP examined the layout of the personnel access building stating that the plan lacked detail. They described the basic security functions to be carried out in that location and also the equipment receiving area. I expect that the security considerations for the personnel and equipment access buildings will be a major part of a site-specific security case. I would expect the licensee to examine these buildings early in the site-specific phase of the project as part of developing their security case.

183. The RP has correctly examined door schedules for evacuation routes and safety related activities. They have identified several occasions when door openings do not necessarily reflect security RGP. The design of doors would be normal business for a licensee. I would therefore expect this matter to be addressed in the site-specific phase and be captured in the development of the security case.

4.5.6 Strengths

184. In my assessment I judge these are strengths:

- The RP has presented a detailed picture of a high-level conceptual security framework through a comprehensive set of documents thereby meeting the general expectations for GDA. In that way they have provided the licensee with the context on which to develop its security case and plan.
- The RP has adopted an intelligent application of SyAPs and focused on the relevant KSyPPs. They have considered the SyAPs-based ‘outcomes’ and related ‘postures’ that would inform the licensee’s security plan development.
- For a conceptual design, the RP has drawn from RGP and specifically CPNI for adversary capability and security doors together with the related performance levels.
- The RP has provided a balanced and integrated approach to all risks whether cyber or physical. In this GDA, the RP has provided a full analysis of cyber risks and mitigation leading to relatively detailed requirements. This is considered coherent with similar analysis conducted in the C&I specialist area. The fact that the RP has conducted joint security and C&I work, and through its collaboration with ONR, is evidence of this ‘joined-up’ approach that sets the bar for interaction in future GDAs.
- The RP has taken adequate steps within GDA to deconflict their security conceptual design with safety measures.
- For GDA, I judge that the RP understands ‘secure by design’ and has applied it realistically to inform their conceptual design.

4.5.7 Outcomes

185. The RP has met my expectations for a meaningful GDA presenting the licensee with a comprehensive framework on which to build their detailed requirements and consider the site as a whole.

186. I have identified areas that I intend to track into licensing being topics of specific regulatory interest. I have identified in this section one AF and several minor shortfalls in my assessment at para 4.5.5.

4.5.8 Conclusion

187. Based on the outcome of my assessment of the SA/SI and CONOPs documents, I conclude that the RP has explained, in an adequate way, how their security conceptual design is underpinned by detailed risk analysis from both physical and cyber security perspectives. Risk-based methodologies have been devised drawing from RGP, then applied to the design thereby offering modifications where possible. When such modifications are not possible, or do not address the risk sufficiently, then the RP has offered a conceptual framework, consistent with KSyPPs and relevant SyAPs, for the licensee to adopt and develop further with confidence. Drawing on the relevant TAGs and other RGP, I am satisfied that this aspect of the GSR would sufficiently inform and shape the relevant aspects of the licensee's security plan. I have raised one AF and identified several minor shortfalls.

4.6 Consolidated Security Case

4.6.1 Assessment

188. Within GDA, expectations for the GSR and security case are explained within the Guide to Requesting Parties (Ref. 1). The GSR is expected to inform the licensee's development of a security plan during the site-specific phase of the project that will meet regulatory expectations. Those expectations are described (not prescribed) in SyAPs (Ref. 2). The security case is different from the safety case although the latter informs security risk analysis that in turn identifies areas that require proportionate protection. Such risk analysis also identifies elements of the design that present security vulnerabilities that might be designed-out after careful consideration. This approach, that requires close safety and security collaboration, is referred to as 'secure by design'. The RP has correctly followed this expectation by placing 'secure by design' at the centre of its case.

189. The security case, captured within the GSR, is described by the RP in a tiered approach (see para 40). The structure for their GSR reflects the logic of SyAPs that are complementary to SAPs (Ref. 8). The RP has adopted a logical approach that examines the design for security vulnerabilities then seeks to first design-out these or, if not achievable, offers a protective security solution that draws from RGP. The GSR Tier 1 document suitably describes the case, adopts a 'secure by design' approach and provides an effective guide to navigating the RP's Tier 2 and 3 documents that provide the necessary evidence for GDA. The security case is argued from 'first principles' given that the reference design is not predicated on the UK DBT and a SyAPs based approach.

190. The RP's Tier 2 document set takes the plant design, the UK DBT (Ref. 10) and draws from RGP to explain their methodology for assessing the risk. The Tier 2 reports include both the CSRAR (Ref. 19) and the VAI&C (Ref. 17) methodologies. Both methodologies draw from respective RGP and their application and outcomes are described in the CSRAR (Ref. 20) and VAI&C Report (Ref 18). The RP has met my expectations by addressing the generic design risk through methodologies drawing from RGP that adequately inform the next step, the conceptual security regime.

191. The RP's risk assessments and reports then successfully inform the conceptual security regime captured in the SA/SI (Ref. 21) and CONOPs (Ref. 22) documents. Both documents reference RGP and provide a realistic level of detail for the licensee to develop in the site-specific phase. The level of detail provided to the licensee, in terms of protection against cyber based risks against known CI&CS, is greater than for physical protection. For protection against non-cyber threats, these documents present a suitable framework that would in turn inform the licensee's security plan.

192. My assessment has been consistent with DR 2.2. I am content that the RP has consolidated its submissions throughout GDA. The RP has also provided me with sufficient confidence that its next submissions will be aligned, and consolidated, to DR3.

4.6.2 Strengths

193. The RP's GSR meets the expectations for GDA in that it addresses SyAPs and would therefore suitably inform a licensee's security plan. Taking such a SyAPs based approach is new to GDA and therefore the RP did not have any experience on which to inform its approach. The suite of documents that collectively forms the GSR contains a suitable level of detail and takes a SyAPs based approach to managing security risk. By focusing on the KSyPPs, the GSR reflects RGP for civil nuclear security as they relate to making a security case. The RP has also taken a holistic view of security, based again on SyAPs, that includes all risks and then explains how both cyber and physical protection measures are delivered drawing effectively from various RGP. I consider that the RP has gone to significant lengths to ensure that there is suitable coverage of the cyber risks, and their management, that correctly reflects the importance of the C&I and Security interface.

4.6.3 Outcomes

194. The RP has identified a number of modifications to the design in applying a 'secure by design' approach. Acknowledging that it is not always feasible to design-out security risk through engineering at this stage in the generic design's development, security infrastructure and architecture needs to be 'designed-in'. The GSR addresses this requirement and therefore provides a suitable framework for a licensee to develop a more detailed security plan in the site-specific phase of the project.

4.6.4 Conclusion

195. I conclude that the GSR, with its tiered approach, meets expectations for GDA in that it provides a meaningful level of detail in its risk analysis and the RP's description of mitigating measures, based on RGP. It is also appropriately aligned with SyAPs-based 'outcomes' within the context of GDA. Therefore, the GSR documents collectively set the conditions for a licensee to develop the security case and adequately inform the arrangements for requirements management in the site-specific phase of the project. I am content that the DR 2.2 based submission reflects my assessment.

4.7 Comparison with Standards, Guidance and Relevant Good Practice

196. Throughout the Security GDA process, the RP has submitted documents which refer to the appropriate legislation, SyAPs and RGP for security protection. In that way they have produced a GSR that would set the conditions for a licensee to develop a site-specific security plan.

197. SyAPs, and an outcome focused regulatory approach, is new to the civil nuclear industry. The related ideas on 'secure by design', as a KSyPP, is equally novel and a developing area of security regulation. The RP has, drawing from expertise in the supply chain, been able to take existing RGP then developing it further and has done

so intelligently. Through the RP's integration into a modification process, they have been able to affect the design early on that mirrors a 'secure by design' approach.

198. The key SyAPs relevant to GDA are the KSyPPs, FSyP 6 (PPS) and 7 (CS&IA). The RP has structured its analysis and reports around these principles. These SyAPs principles are based on a risk-based approach thereafter the application of security industry RGP such as 'defence in depth'. These principles describe the need for risk-based assessments, the application of a 'secure by design' approach and a framework for delivering the appropriate mitigation. The RP's choice of structure for the GSR, with its three tiers, reflects this approach, its logic and captures the idea behind a 'golden thread' from identifying security vulnerabilities to their reduction through applying a SyAPs based approach.

199. Given the complementary relationship between safety and security, ONR SAPs (Ref. 8), have also informed the RP's security case.

200. The RP has made use of these high-level documents:

- IAEA - Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5). (Ref. 9).
- The UK Design Basis Threat (Ref. 10).
- IAEA Technical Guidance document (NSS No 16) 'Identification of Vital Areas at Nuclear Facilities' (Ref. 9).
- The NCSC standards, guidance, and principles documents (Ref. 11),
- IEC standards 27005, 62645, 62443 (Ref. 12)
- IAEA Computer Security of Instrumentation and Control Systems at Nuclear Facilities. Nuclear Security Series No. 33-T (Ref. 9)
- ONRs Security Assessment Principles for the Civil Nuclear Industry Version 0 (Ref. 2).

201. The RP has used standards albeit noting that the licensee will develop systems and equipment through their requirements management. For example, they refer to PAS 68 (Ref. 48) when explaining HVM. The RP explains, in some detail, the MFES (Ref. 47) test ratings as they relate to doors, hatches and vents offering some performance classifications.

202. Overall, I am content that the RP has demonstrated sufficient compliance with relevant standards, guidance and RGP during GDA.

5 CONCLUSIONS AND RECOMMENDATIONS

5.1 Conclusions

203. This report presents the findings of my security assessment of the generic UK HPR1000 design as part of the GDA process.

204. Based on my assessment, undertaken on a sampling basis, I have concluded the following:

- The RP has drawn on RGP and provided a mature explanation of the security case. They refer to the idea of 'holistic security' by which they have brought both cyber and physical risk management together and adopted, then developed, a 'secure by design' approach. The RP has used the KSyPPs to outline a case that has utility for the licensee.
- From a VAI&C perspective, I am satisfied that the RP has presented sufficient arguments and evidence to substantiate its overarching VAI&C claim that the security threat will be managed to protect the public from the risks arising from a radiological event caused by the theft or sabotage of NM or ORM and supporting systems. The arguments and evidence presented by the RP to support the above claim align with RGP for VAI&C and satisfy the requirements of SyDP 6.2 (Physical Protection Systems, Categorisation for Sabotage).
- I judge that the RP, through the application of its VAI&C methodology, has produced a comprehensive list of categorised VAs to inform protection system requirements. Furthermore, the developed VAI&C methodology incorporates a process of continuous review as new design information is generated through changes to the plant design and threat. This meets my expectations and is consistent with the SyAPs approach.
- Regarding cyber security, for the systems sampled, I consider that they are adequately protected by the security controls within GDA scope. Where controls are outside of the GDA scope, and enabling activities are required, then I also consider the enabling activities sampled as adequate. There are sufficient strategies in place to deliver cyber security assurance and production excellence for cyber security, when supported by an acceptable wider production excellence process.
- Based on the outcome of my assessment of the SA/SI and CONOPs documents (Refs 21 and 22), I have concluded that the RP has explained, in an adequate way, how its security conceptual design is underpinned by detailed risk analysis from both physical and cyber security perspectives. Risk-based methodologies have been devised drawing from RGP, then applied to the design thereby offering modifications where possible. When such modifications are not possible, or do not address the risk sufficiently, then the RP has offered a conceptual framework, consistent with KSyPPs and relevant SyAPs, for the licensee to take on and develop further.
- Drawing on the relevant TAGs and other RGP, I assess that the SA/SI and CONOPs aspects of the GSR would sufficiently inform and shape the relevant aspects of the licensee's security plan. The RP has therefore developed a suitable method to concentrate the most robust security measures against the highest risk targets. This has been completed by the RP whilst acknowledging that it is for the licensee to use such a methodology in deciding what capabilities (structures, systems and components) are necessary to deliver security functions as outlined in SyAPs.

205. Overall, based on my sample assessment of the security case for the generic UK HPR1000 design undertaken in accordance with ONR's procedures, I am satisfied that the case, presented within the GSR, is acceptable. On this basis, I am content that a DAC should be granted for the generic UK HPR1000 design from a Security perspective.

5.2 Recommendations

206. Based upon my assessment detailed in this report, I recommend that:

- **Recommendation 1**: From a Security perspective, ONR should grant a DAC for the generic UK HPR1000 design.
- **Recommendation 2**: The five AFs identified in this report should be resolved by the licensee for a site-specific application of the generic UK HPR1000 design.

6 REFERENCES

1. *New nuclear reactors: Generic Design Assessment: Guidance to Requesting Parties for the UK HPR1000*. ONR-GDA-GD-001. Revision 4. October 2019. ONR. www.onr.org.uk/new-reactors/ngn03.pdf

2. *Security Assessment Principles for the Civil Nuclear Industry*. 2017 Edition, Version 0. March 2017. http://www.onr.org.uk/syaps/security-assessment-principles-2017.pdf

3. *Generic Security Report*. HPR/GDA/GSR/0001. Rev 001. January 2020. GNSL. ONR CM9 Ref 2022/2402.

4. Technical Assessment Guides

   Categorisation for Theft. CNS-TAST-GD-6.1. Rev 1. ONR. April 2020.
   Target Identification for Sabotage. CNS-TAST-GD-6.2. Rev 1. ONR. April 2020.
   Physical Protection System Design. CNS-TAST-GD-6.3. Rev 1. ONR. March 2020. CM9 Ref for O-S:SNI version 2019/135667.
   Effective Cyber and Information Risk Management. CNS-TAST-GD-7.1. Rev 1. ONR. March 2020.
   Protection of Nuclear Technology and Operations. CNS-TAST-GD-7.3. Rev 1. ONR. March 2020.
   Preparation for and Response to Cyber Security Events. CNS-TAST-GD-7.5. Rev 2. ONR. March 2020.
   Guidance on The Security Assessment of Generic New Nuclear Reactor Designs. CNS-TAST-GD-11.1 Rev 0. ONR. June 2017.
   Guidance on Mechanics of Assessment. NS-TAST-GD-096. Rev 0. April 2020.
   http://www.onr.org.uk/operational/tech_asst_guides/index.htm

5. *GDA Step 4 Assessment Plan of the Security topic for the UK HPR1000 Reactor*. ONR-GDA-UKHPR1000-AP-19-017. Revision 0. February 2020. ONR. CM9 Ref 2020/8710.

6. *GDA Step 4 Cyber Security Assessment Strategy for the UK HPR1000 Reactor*. ONR-GDA-UKHPR1000-AP-19-014. Revision 0. February 2020. ONR. CM9 Ref 2020/24624.

7. *Scope for UK HPR1000 GDA Project*. HPR-GDA-REPO-0007. Rev 001. 18 July 2019. GNSL. CM9 Ref 2019/209339.

8. *Safety Assessment Principles for Nuclear Facilities*. 2014 Edition. Revision 1. January 2020. ONR. http://www.onr.org.uk/saps/saps2014.pdf

9. IAEA

   Convention on the Physical Protection of Nuclear Material. IAEA.
   Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5). Nuclear Security Series (NSS) 13. 2011. IAEA.
   Security during the Lifetime of a Nuclear Facility. NSS 36-G. 2019. IAEA.
   Computer Security at Nuclear Facilities. NSS 17. 2011. IAEA.
   Computer Security of Instrumentation and Control Systems at Nuclear Facilities. NSS 33-T. 2018. IAEA.
   Safety of Nuclear Power Plants: Design. Safety Requirements. Safety Standards Series No. NS-R-1. 2000. IAEA.
   https://www-pub.iaea.org

10. *HMG UK Design Basis Threat*. Review 1. November 2019.

11. National Cyber Security Centre (NCSC)

The CPA Build Standard. Ver 1.4. October 2018. NCSC.
https://www.ncsc.gov.uk/files/CPA-Build_Standard_1-4.pdf
Secure Design Principles. Ver 1.0. May 2019. NCSC.
https://www.ncsc.gov.uk/collection/cyber-security-design-principles
Process for Performing Commercial Product Assurance (CPA) Foundation Grade Evaluations. Issue 2.5. October 2018. NCSC.
https://www.ncsc.gov.uk/information/commercial-product-assurance-cpa
Cyber Assessment Framework. Ver 3.0. 30 September 2019. NCSC.
https://www.ncsc.gov.uk/collection/caf/cyber-assessment-framework/
IS1&2 (now deprecated) Risk management guidance
https://www.ncsc.gov.uk/collection/risk-management-collection/component-system-driven-approaches/understanding-component-driven-risk-management

12. International Electrotechnical Commission (IEC)

Nuclear power plants – Instrumentation and control systems – Requirements for security programmes for computer-based systems. IEC 62645. Edition 1.0. 2014.
Nuclear power plants - Instrumentation and control systems - Requirements for coordinating safety and cybersecurity. BS IEC 62859:2016.
Information technology - Security techniques - Evaluation criteria for IT Security. IEC/ISO 15408:2009.
www.iec.ch

13. *Pre-Construction Safety Report*. HPR/GDA/PCSR/0027. Rev 001. 10 January 2020. GNSL. CM9 Ref 2020/13980.

14. *Design & Plant Information*. HPR-GDA-REPO-0069. Rev 001. 3 December 2019. GNSL. CM9 Ref 2019/379720.

15. *Threat Interpretation Document*. HPR-GDA-REPO-0122. Rev 001. 29 January 2021. GNSL. ONR Cheltenham CDR Ref 1/428.

16. *UK Civil Nuclear Sector Cyber Threat Assessment*. 16674-1. Ver 1.1. 23 March 2018. Context IS. CM9 Ref 2018/105002.

17. *UKHPR 1000 Vital Area Identification and Categorisation methodology*. HPR-GDA-REPO-0062 Rev 001. 19 December 2019. GNSL. ONR Cheltenham CDR 1/418.

18. *VAI&C Assessment Analysis*. GDA-REC-RIS-SEC-000021. Tier 3 DR2-2 Issued. Rev 001. 8 April 2021. GNSL. CM9 Ref 2021/29864.

19. *Cyber Security Risk Assessment Methodology*. HPR-GDA-REPO-0108. Rev 001. 27 February 2021. GNSL. CM9 Ref 2021/65561.

20. *Cyber Security Risk Assessment Report*. GDA-REC-GNSL-SEC-000026. Rev 002. 26 January 2021. GNSL. CM9 Ref 2021/29846.

21. *Security Architecture/Security Infrastructure*. HPR-GDA-REPO-0113. Rev 002. 26 January 2021. GNSL. CM9 Ref 2021/29869.

22. *Concept of Operations*. HPR-GDA-REPO-0112. Rev 002. 26 January 2021. GNSL. CM9 Ref 2021/29867.

23. *Security GDA TAG – Additional Notes*. 30 April 2020. ONR. CM9 Ref 2020/104393.

24. *GSR 0002 Revision 0 and Tier 2 Documents Comments*. April 2020. ONR. CM9 Ref 2020/55027 & 2020/55023.

25. *Table of Contents for Generic Security Report - Security Case (Version 2).* HPR-GDA-GSR-0001. Rev 001. GNSL. CM9 Ref 2021/44471.

26. *Register of GSR Changes*. GDA-REC-GNSL-008504. Version 2. 28 May 2021. GNSL. CM9 Ref 2021/44470.

27. *ONR GNSL GSR Security L4 KIT*. 22 July 2021. GNSL. CM9 Ref 2021/54783.

28. *Annex A Nuclear Inventory DR2-2 Issued*. GDA-REC-RIS-SEC-000021. Rev 002. 8 April 2021. GNSL. CM9 Ref 2021/29844.

29. *Annex B Inventory Assessment DR2-2 Issued*. GDA-REC-RIS-SEC-000021. Rev 002. 26 January 2021. GNSL CM9 Ref 2021/11719.

30. *Annex C IEMOs. potential targets and PSECs DR2-2 Issued*. GDA-REC-RIS-SEC-000021. Rev 002. 8 April 2021. GNSL. CM9 Ref 2021/29851.

31. *Annex D Location Analysis DR2-2 Issued*. GDA-REC-RIS-SEC-000021. Rev 002. 8 April 2021. GNSL. CM9 Ref 2021/29858.

32. *Annex E: Threat assessment*. GDA-REC-RIS-SEC-000021. Rev 002. 8 April 2021. GNSL. ONR Cheltenham CDR Ref 1/427.

33. *Annex F Theft Assessment DR2-2 Issued*. GDA-REC-RIS-SEC-000021. Rev 002. 8 April 2021. GNSL. CM9 Ref 2021/29861.

34. *Annex G - Vital Areas and Categorisation DR2-2 Issued*. GDA-REC-RIS-SEC-000021. Rev 002. 8 April 2021. GNSL. CM9 Ref 2021/29862.

35. *Annex H Basis of Assessment DR2-2 Issued*. GDA-REC-RIS-SEC-000021. Rev 002. 8 April 2021. GNSL. CM9 Ref 2021/29863.

36. *GDA Step 3 Assessment of Security for the UK HPR1000 Reactor*. ONR-NR-AN-19-013. Revision 0. 8 January 2020. ONR. CM9 Ref 2019/355531.

37. *UK HPR1000-Regulatory Observations (RO) Tracking Sheet*. ONR. CM9 Ref 2019/465031.

38. *UK HPR1000 Vital Area Categorisation and Classification Methodology*. HPR-GDA-REPO-0121. Rev 001. 26 October 2019. GNSL. CM9 Ref 2019/281912.

39. *Vital Area Report (Tier 2) DR2-2 Issued*. HPR-GDA-REPO-0107. Rev 003. 26 January 2021. GNSL. CM9 Ref 2021/29866.

40. *Step 4 Control and Instrumentation Assessment of the UK HPR1000 Reactor*. ONR-NR-AR-21-005. Revision 0. ONR. CM9 Ref 2021/46296.

41. *Cyber Security Design Requirements Specification (CSDRS).* HPR-GDA-SPEC-0114. Rev 001. 12 March 2021. GNSL. CM9 Ref 2021/21834.

42. *ONR TSC C&I Support for General Nuclear Systems UK HPR1000 GDA Step 4 - Evidence and Adequacy of C&I Architecture - Appendix A Cyber Security, S.P1893.041.07 - Appendix A*. Issue 1.0. August 2021. Capgemini Engineering. CM9 Ref 2021/60561.

43. *Cyber Security for Industrial Automation and Control Systems (IACS).* OG86. Edition 2 HSE. https://www.hse.gov.uk/foi/internalops/og/og-0086.pdf

44. *UK HPR1000 - Regulatory Query (RQ) Tracking Sheet*. ONR. CM9 Ref 2017/407871.

45. *Step 4 Cyber Security & Information Assurance Assessment of the UK HPR1000 Reactor*. ONR-NR-AN-21-014. Rev 0. 12 July 2021. ONR. CM9 Ref 2021/44510.

46. *Implementing Secure by Design at Nuclear Facilities*. Version 4.1. March 2019. World Institute for Nuclear Security (WINS). https://www.wins.org/document/4-1-security-by-design/

47. *CPNI Product Rating System. Manual Forced Entry Standard Part 1.* April 2015. CPNI. https://www.cpni.gov.uk/protection-forced-entry

48. *BSI - PAS 68 - Impact test specifications for vehicle security barrier*. June 2019. CPNI. Advice Note - Due Diligence in selecting barriers - 03 March 2020 v3.pdf (cpni.gov.uk)

Annex 1

Relevant Security Assessment Principles Considered During the Assessment

SyAP No	SyAP Title	Description
6	Fundamental Security Principle 6: Physical Protection Systems	A proportional physical protection system that integrates technical and procedural controls to form layers of security that build ‘defence in depth’ and are graded according to the potential consequence of a successful attack.
7	Fundamental Security Principle 7: Cyber Security & Information Assurance	The requirement to implement and maintain effective cyber security and information assurance arrangements that integrate technical and procedural controls to protect the confidentiality, integrity and availability of SNI and technology.
6.1	Categorisation for Theft	The requirement to undertake a characterisation of a plant, site or facilities in order to determine the categorisation for theft.
6.2	Categorisation for Sabotage	The requirement to undertake a characterisation of a plant, site or facilities in order to determine the categorisation for sabotage.
6.3	Physical Protection System Design	The requirement to design and implement a physical protection system that builds ‘defence in depth’ and meets the required security ‘outcome’ based on the categorisation for theft and sabotage.
7.1	Effective Cyber and Information Risk Management	The need to maintain arrangements to ensure that CS&IA risks are is managed effectively.
7.3	Protection of Nuclear Technology and Operations	The need to ensure their operational and information technology is secure and resilient to cyber threats by integrating security into design, implementation, operation and maintenance activities.
7.5	Preparation for and Response to Cyber Security Incidents	The need to implement well-tested plans, policies and procedures to reduce their vulnerability to cyber security incidents (especially from the most serious threats of terrorism or cyber-attack), non-malicious leaks and other disruptive challenges.
1-6	Key Security Plan Principles	The principles apply across a wide range of facilities of differing type and categorisation for theft and sabotage. Applying these principles therefore requires judgement and proportionality in deciding which principles are relevant to the situation being assessed and then whether enough has been done in relation to each applicable principle.

SyAP No	SyAP Title	Description
KSyPP 1	Secure by Design	'Secure by Design' is an approach that seeks to reduce vulnerabilities rather than attempting to secure or mitigate them post design. It mitigates specific threats by using an approach, design or arrangement tailored to address malicious acts.
KSyPP 2	The Threat	Protection systems should be designed, evaluated and tested using the state's Design Basis Threat (DBT). It is essential that a DBT is used as the basis for the design, evaluation and testing of protection systems to seek assurance that it will meet a defined security 'outcome' depending on the maturity of a design. Within the UK, the DBT malicious capabilities assessed as confronting the civil nuclear industry and assumptions about the composition and capabilities of terrorist groups and others posing a threat are described in detail in UK Government planning assumptions.
KSyPP 3	The Graded Approach	Protection systems should be based on a graded approach, considering the categorisation for theft or sabotage of NM/ORM, and consequence of compromise of any SNI.
KSyPP 4	Defence in Depth	Protection systems should reflect a concept of several layers and methods of protection that have to be overcome or circumvented by an adversary and ensure appropriate mitigation of security events should prevention fail.
KSyPP 5	Security Categorisation and Classification	The security functions to be delivered within any conceptual design, in all modes of operation, should be identified and then categorised based on their significance. With regard to security structures, systems and components that have to deliver such security functions they should be identified and classified on the basis of those functions and their significance to security.
KSyPP 6	Codes and Standards	Structures, systems and components that are important to security should be designed, manufactured, constructed, installed, commissioned, quality assured, maintained, tested and inspected to appropriate codes and standards.

Annex 2

Assessment Findings

Note: These Assessment Findings must be read in the context of the sections of the report listed in this table, where further detail is provided regarding the matters that led to the findings being raised.

Number	Assessment Finding	Report Section
AF-UKHPR1000-0047	The licensee shall complete cyber security compliance analysis for all computer-based C&I systems important to safety and implement measures to address all instances of partial or non-compliance.	4.4.2
AF-UKHPR1000-0054	The licensee shall, as part of detailed site-specific design, demonstrate that the security controls identified in each of the cyber security risk assessments have been considered against the core platform/component delivering the safety/security function. Peripheral components (for example maintenance workstations) must also have suitable security controls selected based on the threat they pose to the core platform/component.	4.4.2
AF-UKHPR1000-0046	The licensee shall resolve the residual cyber security vulnerabilities identified in the GDA cyber security risk assessment report as part of detailed design. This should include the potential modifications proposed during GDA.	4.4.3
AF-UKHPR1000-0045	The licensee shall, as part of detailed design of the C&I systems, develop the cyber security risk assessment to include all C&I systems important to safety, and all interfaces between and within those systems. The assessment should follow a methodology that is at least as rigorous as that developed for GDA, and should include demonstration that measures are in place to address all identified vulnerabilities.	4.4.3

Number	Assessment Finding	Report Section
AF-UKHPR1000-0055	The licensee shall, as part of site-specific detailed design, identify the facilities, equipment and support necessary for the security system. It should be a priority to secure sufficient space and support for the security equipment and activities, and to integrate and deconflict it with other plant systems, so to deliver the security outcomes sought as part of the site-specific security case.	4.5.5