Office for Nuclear Regulation

New Reactors Division

Step 4 Assessment of Conceptual Security Arrangements for the UK Advanced Boiling Water Reactor

Assessment Report: ONR-NR-AR-17-026
Revision 0
December 2017

EXECUTIVE SUMMARY

Hitachi-GE Nuclear Energy Ltd is the designer and GDA Requesting Party for the United Kingdom Advanced Boiling Water Reactor (UK ABWR). Hitachi-GE commenced Generic Design Assessment (GDA) in 2013 and completed Step 4 in 2017.

This assessment report is my Step 4 assessment of the Hitachi-GE UK ABWR reactor design in the area of security.

The scope of my assessment is to review the security aspects of the UK ABWR in greater detail, by examining the evidence supporting the claims and arguments made in the UK ABWR Conceptual Security Arrangements (CSA) document and building on the assessments already carried out for Step 3. In addition, I have provided a judgement on the adequacy of the information contained within the Conceptual Security Arrangements document.

Throughout the GDA process, my assessment was undertaken against the National Objectives, Requirements and Model Standards (NORMS). NORMS was replaced in March 2017 with ONR's Security Assessment Principles (SyAPs). I continued to undertake my assessment against NORMS rather than change strategy in the final stages of GDA. This approach aligns with my Step 4 plan and the phased adoption of SyAPs across industry. It is important that a future licensee builds on the CSA to develop a site specific security plan which is compatible with SyAPs.

A crucial area in the development of the CSA is the identification of assets which require protection. A significant part of Hitachi-GE's CSA has been the development and application of an appropriate methodology to determine those assets which require protection from sabotage and theft. This identification acts as a basis for developing graded and proportionate security arrangements.

My assessment conclusion is:

- I am satisfied with the claims arguments and evidence laid down within the Conceptual Security Arrangements submitted as part of the GDA process.
- I consider that from a security viewpoint, the Hitachi-GE UK ABWR design is suitable for construction in the UK subject to approval of relevant security plans.

My judgement is based upon the following factors:

- Hitachi-GE has adequately categorised nuclear and other radioactive material against theft.
- Hitachi-GE has adopted a robust and comprehensive methodology to identify critical assets (including Computer Based Systems Important to Safety) and vital areas which include structures, systems and components (SSCs).
- Hitachi-GE has adequately identified those assets requiring protection and applied a systematic approach to grading those assets based on potential unacceptable radiological consequences resulting from sabotage.
- Hitachi-GE has developed a proportionate physical protection solution using recognised security standards that provide a graded approach to protecting identified assets, also demonstrating the principle of defence in depth to meet NORMS security objectives
- Hitachi-GE has adequately demonstrated that safety requirements have been considered when developing security arrangements.

The following matters remain, which are for a future licensee to consider and take forward in their site-specific security submissions. These matters do not undermine the CSA but require licensee input/decision at a specific site:

- Modifications to plant design will require a re-evaluation of the Vital Area (VA) status. Late design changes to some areas of the plant have been taken into account by Hitachi-GE and a conservative re-evaluation undertaken which has identified *potential* VAs. In addition, some VAs were identified using generic data, and conservative assumptions made. These VAs should be re-evaluated using site specific data to confirm or otherwise VA status. The identified anomalies relating to the VAs in the CSA appendices should be reviewed and corrected.

- The cyber analysis undertaken by Hitachi-GE used a combination of deterministic and probabilistic analyses based on the most capable of threat actors, which was considered adequate for GDA as it supports the evidence related to the overall architecture of the safety systems. A broader risk assessment covering the full range of threat actor capability will need to be adopted by the licensee once site specific technology has been chosen and when developing the site security plan.

- Provision of back-up power supply to security systems has not been determined by Hitachi-GE. The licensee shall identify the requirement for, and provision of power to the site security systems in order to minimise the risk of power failure.

To conclude, I am satisfied with the claims, arguments and evidence laid down within the CSA. I consider that from a security view point, the Hitachi-GE UK ABWR design is suitable for construction in the UK subject to future permissions and permits being secured.

LIST OF ABBREVIATIONS

ASCE	American Society of Civil Engineers
C&I	Control & Instrumentation
CBSIS	Computer Based Systems Important to Safety
CA	Critical Asset
CCTV	Closed Circuit Television Vision
CPPNM	Convention on the Physical Protection of Nuclear Materials
CNI	Critical National Infrastructure
CNS	Civil Nuclear Security
CPNI	Centre for the Protection of the National Infrastructure
CSA	Conceptual Security Arrangements
CS&IA	Cyber Security & Information Assurance
CSISy	Computer Systems Important to Security
DAC	Design Acceptance Confirmation
DAG	Diverse Alternate Generator
DBT	Design Basis Threat
EA	Environment Agency
EDG	Emergency Diesel Generator
FPGA	Field Programmable Gate Array
GDA	Generic Design Assessment
HWBS	Hard-wired Back-up System
IAEA	The International Atomic Energy Agency
IPS	Integrated Protection Solution
LOOP	Loos of Off-site Power
NIMCA	Nuclear Industries Malicious Capabilities (Planning) Assumptions
NISR 2003	Nuclear Industries Security Regulations 2003
NORMS	National Objectives, Requirements and Model Standards
NSSP	Nuclear Site Security Plan
NM	Nuclear Material
NRW	Natural Resources Wales
ONR	Office for Nuclear Regulation
ORM	Other Radioactive Material
OT	Operational Technology
PCntlS	Plant Control System
PIDS	Perimeter Intruder Detection System

PPS	Physical Protection System
PSM	Protective Security Measures
RCA	Radiologically Controlled Area
RI	Regulatory Issue
RO	Regulatory Observation
RQ	Regulatory Query
RP	Requesting Party
SINS	Security Informed Nuclear Safety
SME	Subject Matter Expert
SMS	Security Management System
SNI	Sensitive Nuclear Information
SoDA	Statement of Design Acceptability
SSC	System, Structure (and) Component
SSCR	Site Security Control Room
SSLC	Safety System and Logic Controller
SyAPs	Security Assessment Principles
TAG	Technical Assessment Guide
TSC	Technical Support Contractor
UK ABWR	United Kingdom Advanced Boiling Water Reactor
UPS	Uninterruptable Power Supply
URC	Unacceptable Radiological Consequence
VA	Vital Area
VAI	Vital Area Identification

TABLE OF CONTENTS

Table(s)

Annexes

1 INTRODUCTION

1.1 Background

1. Information on the GDA process is provided in a series of documents published on the ONR website: http://www.onr.org.uk/new-reactors/index.htm. The outcome from the GDA process sought by Requesting Parties such as Hitachi-GE is a Design Acceptance Confirmation (DAC) for ONR and a Statement of Design Acceptability (SoDA) for the Environment Agency (EA) and Natural Resources Wales (NRW).

2. The GDA Step 3 summary report is published on our website (**http://www.onr.org.uk/new-reactors/uk-abwr/reports/step3/uk-abwr-step-3-summary-report.pdf**). Further information on the GDA process in general is also available on our website (**http://www.onr.org.uk/new-reactors/index.htm**).

3. The GDA of the UKABWR has followed a step-wise approach which commenced in 2013. Major interactions started in Step 2 with an examination of methodology adopted to identify VAs and understand overall concept of security employed. This continued through Step 3 with identification of candidate VAs and application of the UK design basis threat (DBT). The Step 4 assessment is an in-depth assessment of the safety, security and environmental evidence. Through the review of information provided to ONR, the Step 4 process should confirm that Hitachi-GE:

   - Has properly justified the higher-level claims and arguments.
   - Has progressed the resolution of any issues identified during Step 3.
   - Has provided sufficient detailed anaysis to allow ONR to come to a judgment of whether a DAC can be issued.

4. During the Step 4 assessment I have undertaken a detailed assessment, on a sampling basis of the evidence provided within the Conceptual Security Arrangements (CSA) document (Reference 1). My assessment has included but not been limited to taking into account those areas relating to VA identification and CBSIS examined by relevant ONR inspectors and reported upon accordingly. The full range of items that might form part of the assessment is provided in ONR's GDA Guidance to Requesting Parties (Reference 2). These include:

   - Consideration of issues identified in Step 3.
   - Ensuring the correct facility categorisation against theft and sabotage has been carried out.
   - Judging the design against the National Objectives, Requirements and Model Standards (NORMS) (Reference 3).
   - Reviewing Hitachi-GE's methodology and its application for the identification of Vital Areas.
   - Establishing whether the security arrangements provide adequate mitigation of design basis threats as described in the extant Nuclear Industries Malicious Capabilities Planning Assumptions (NIMCA) (Reference 4).
   - Resolution of any identified nuclear security issues, or identifying paths for resolution.

5. This is my assessment report from the ONR's Step 4 assessment of the Hitachi-GE UK ABWR design in the area of security.

6. While a number of Regulatory Queries (RQs) have been raised throughout Step 4 to request clarification and expand on certain areas, no Regulatory Observations (ROs) or Regulatory Issues (RIs) have been raised in the area of security.

7. To ensure this report provides for a comprehensive record of the security assessment, Sensitive Nuclear Information (SNI) has been included at Annex 1. The information has been classified in line with the Classification Policy for the Civil Nuclear Industry (Reference 5). Annex 1 will not be included in the published version of this report but will be made available to the Requesting Party (RP).

1.2 Scope

8. In the earlier Steps 2 and 3 of the GDA, the focus of my assessment was on the approach and methodology taken to identify those assets requiring protection resulting in the identification of candidate VAs. The assessment strategy for GDA Step 4 in the security area was set out in my Step 4 Assessment Plan ONR-GDA-AP-15-014 (Reference 6). The scope of the Step 4 assessment continued to focus on the identification of NM, ORM and SSCs including Operational Technology (OT) that require protection, and particularly the application of the UK DBT to confirm or otherwise the VA status of those areas identified as candidate VAs in Step 3. Step 4 also focussed on the measures that will be designed into the plant to form an integral part of the overall security infrastructure to prevent sabotage or theft of nuclear or other radioactive material and sabotage of nuclear facilities, and ensure the security of equipment and software used or stored in connection with activities involving Nuclear Material.

9. There are matters relevant to security that cannot be adequately assessed during GDA as they are directly related to the operating regimes and associated barriers and security systems to be determined by the licensee but which will be essential to provide defence-in-depth to address internal (insiders[1]) and external threats. These measures include site specific physical arrangements such as perimeter fences, site access arrangements, ongoing personnel security arrangements (aftercare), guards and response forces in addition to comprehensive security procedures and instructions.

10. The scope of my assessment is appropriate for GDA because it has included all areas of the nuclear island where nuclear or other radioactive material is held or stored and included those SSCs essential to preventing unacceptable radiological consequences. It is aligned with those relevant aspects of NORMS which are not site specific or need the input of a future licensee.

1.3 Method

11. My assessment complies with internal guidance on the mechanics of assessment within ONR:

- Guidance on the Security Assessment of Generic New Nuclear Reactor Designs (Technical Assessment Guide CNS-TAST-GD-007).

2 ASSESSMENT STRATEGY

2.1 Standards and criteria

12. The standards and criteria adopted within this assessment are principally the National Objectives, Requirements and Model Standards (NORMS) for the Protective Security of Civil Licensed Nuclear Sites, Other Nuclear Premises and Nuclear Material in Transit, internal Technical Assessment Guides, relevant national and international standards and relevant good practice informed from existing practices adopted in the UK.

---

[1] *IAEA Nuclear Security Series No 8 – the term 'insider' is used to describe an adversary with authorised access to a nuclear facility, a transport operation or sensitive information.*

13. The security standards in NORMS are offered as a benchmark (i.e. Model Standards) to reflect internationally agreed recommendations on the physical protection of NM published by the IAEA in the extant version of INFCIRC/225 (Reference 7). These standards also reflect the United Kingdom's obligations under the Convention on the Physical Protection of Nuclear Materials (CPPNM) (Reference 8). Site specific security arrangements will be assessed as part of the licensee's Nuclear Site Security Plan (NSSP) submission.

14. My assessment focuses on those conceptual security arrangements put in place to protect the public, workforce and environment from the risks arising from a radiological event caused by the theft or sabotage of Nuclear Material or Other Radioactive Material and supporting systems or through the compromise of Sensitive Nuclear Information.

2.1.1 NORMS v ONR Security Assessment Principles

15. ONR's Security Assessment Principles (SyAPs) (Reference 9) constitute the regulatory principles against which dutyholders' security plans are assessed. ONR SyAPs were introduced on 31 March 2017, replacing the NORMS for the Protective Security of Civil Licensed Nuclear Sites, Other Nuclear Premises and Nuclear Material in Transit.

16. With the introduction of SyAPs towards the end of Step 4 of the UKABWR GDA, I considered it reasonable to continue to undertake my assessment against NORMS rather than change strategy in the final stages of GDA. This aligns with my Step 4 assessment plan and the phased adoption of SyAPs across the civil nuclear industry. I took this decision with full agreement of Hitachi-GE and this strategy has been acknowledged in the CSA under the Regulatory Assessment Reference Document (Section 4). With this in mind, it is expected that a licensee will build on the CSA to develop a site specific security plan which is compatible with the expectations set out in the SyAPs. It should be noted that the identification of assets, specifically categorisation for theft and sabotage, has not changed between NORMS and SyAPs. Similarly the security outcomes described in SyAPs, to be achieved for particular categories of material and SSCs, match those achieved by fulfilment of the objectives, requirements and model standards in NORMS.

17. NORMS have been used in the assessment of the UK ABWR conceptual security arrangements:

- Part One – General Requirements
- Part Two - Protecting Nuclear and Other Radioactive Material (including Radioactive Sources) From Theft.
- Part Three – Protecting Vital Areas from Sabotage
- Other relevant sub-sections

18. In assessing Hitachi-GE's application of the graded approach to security arrangements, NORMS objectives in relation to the categorisation of nuclear material for theft and the consequence of sabotage have underpinned my assessment. I have sought to ensure that appropriate evidence has been provided by Hitachi-GE to underpin its arguments in meeting those objectives.

2.1.2 Technical Assessment Guides

19. The Technical Assessment Guides (TAGs) that have been used as part of this assessment are set out in Annex 3.

2.1.3 Technical Advice

20. ONR's Security Informed Nuclear Safety (SINS) Inspectors provide technical advice to support security assessments. Safety Inspectors working within SINS have assessed the adequacy of Hitachi-GE's Vital Area identification process and reported on it accordingly at Reference 10. A synopsis of their report is available to Hitach-GE at Annex 1.

21. ONR's Cyber Security and Information Assurance (CS&IA) inspectors provide technical advice on Operational Technology (OT) including Computer Based Systems Important to Safety (CBSIS). CS&IA Inspectors have undertaken assessment of the OT and Hitachi-GE's overarching cyber security case, and reported upon the findings in Reference 11, a synopsis of which is included at Annex 2.

22. The observations and findings of the technical advice are reflected in this report.

2.1.4 National and international standards and guidance

23. The International Atomic Energy Agency (IAEA) sets out internationally agreed recommendations on the physical protection of nuclear material and nuclear facilities, published in the extant version of INFCIRC/225 as part of the Nuclear Security Series publications. The security standards in NORMS are offered as a benchmark against these recommendations and reflect the United Kingdom's obligations under the CPPNM. Therefore, through assessing Hitachi-GE's submissions against the NORMS, it can be inferred that international guidance is being met.

24. The Centre for the Protection of the National Infrastructure (CPNI) is the UK's national security authority for protective security advice to the UK national infrastructure. CPNI evaluate security products for use in the Critical National Infrastructure and Government, and apply a grading system to rate products against surreptitious and forcible attacks. CPNI also provide resource, guidance and advice in all aspects of security which can be considered and drawn upon as relevant good practice. I have used these standards to assess Hitachi-GE's conceptual security arrangements dealing with physical security measures.

2.2 Technical Support Contractors (TSCs)

25. There were no Technical Support Contractors used in the topic stream for security.

2.3 Integration with other assessment topics

26. The GDA process requires the submission of an adequate, coherent and holistic generic safety and security case. Regulatory assessment cannot therefore be carried out in isolation as there are often safety issues of a multi-topic or cross-cutting nature that impact on security requirements and vice versa. The following cross-cutting issues have been considered within this assessment:

- **Conventional Fire Safety**. The configuration of evacuation routes, emergency exits and fire doors can impact on security particularly access control and the prevention of unauthorised entry into sensitive areas. This assessment report has considered those safety requirements, their impact on security and the resolution of any conflicts to ensure both safety and security requirements can be met.

- **Controls and Instrumentation (C&I)**. The identification of CBSIS and application of security measures has required close coordination with C&I Inspectors, particularly in assessing C&I architectures relevant to security.

- **Electrical Power**. There are claims within the CSA regarding the provision of power to the security systems in both normal operations and during loss of off-site power. Hitachi-GE's evidence for the supply of power to security systems has been reviewed and commented on by ONR's inspector assessing the design's electrical power system.

2.4 Sampling strategy

27. It is seldom possible, or necessary, to assess a security case in its entirety, therefore sampling is used to limit the areas scrutinised, and to improve the overall efficiency of the assessment process. Sampling is done in a focused, targeted and structured manner with a view to revealing any topic-specific or generic weaknesses in the security case.

28. The sampling strategy for this assessment was to ensure suitable and robust methodologies were employed to identify Vital Areas, CBSIS and to facilitate the categorisation of the design for theft and sabotage. Once these key areas were satisfactorily addressed, my focus turned to the application of defence in depth to ensure appropriate protection was applied to mitigate design basis threats against both theft and sabotage. The objectives detailed in NORMS relating to theft and sabotage acted as a basis for the assessment. A number of key buildings, floors and sensitive areas were examined to ensure that the defence in depth principles were appropriately applied. These were:

- Reactor Building
- Control Building
- Radwaste Building
- Turbine Building
- Services Building
- Filter Vent Building
- Back-up Building
- Service Tunnels
- Heat Exchanger Building
- Emergency Diesel Generators

Overall I assessed the security arrangements associated with the above buildings including access control, detection and delay and sampled the arrangements on a number of floors and sensitive areas within those buildings.

2.5 Out of scope items

The following table sets out those items which have been agreed with Hitachi-GE as being outside the scope of GDA.

Out of Scope	Rationale
Site specific security measures	These will be determined by the licensee based on site specific factors such as number of units to be deployed, perimeter configuration, and guard and response force arrangements. They will be assessed by ONR as part of the licensee's security submissions.
Site Security Control Room and alternate.	Location and configuration will be determined by the licensee and assessed by ONR as part of the licensee's security submissions

Spent Fuel Interim Store	The lack of any detailed design of an SFIS precluded a security assessment. Any future design will require full security assessment to demonstrate compliance with SyAPs.

Table 1

2.6 Protection of Sensitive Nuclear Information

29. The main body of this report is "OFFICIAL" information and deemed releasable to the public. A limited amount of Sensitive Nuclear Information (SNI)[2] has been included in Annex 1 to provide for a comprehensive record of the assessment undertaken. This information has been categorised in line with the Classification Policy for the Civil Nuclear Industry. In accordance with Section 79 of the Anti-terrorism, Crime and Security Act (Reference 12), the information in this Annex is not made available to the public and has been removed from the publically accessible version of the report.

[2] *As defined in Section 77(7) of the Anti-terrorism, Crime and Security Act 2001*

3 REQUESTING PARTY'S CSA

30. Hitachi-GE has submitted its CSA as the principal document outlining its claims, arguments and evidence for the security of the UK ABWR to operate within Great Britain. The CSA presents the overarching security position for the closeout of the GDA process.

31. Hitachi-GE has identified potential targets for unauthorised removal of nuclear material and for sabotage. This has been done through examining NM and ORM inventories and identification of critical assets (CAs) and vital areas (VAs). Hitachi-GE has applied the UK DBT as defined in the extant version of NIMCA to identify potential vulnerabilities and design protective security measures. This information has been consolidated and documented within the UK ABWR CSA.

32. Hitachi-GE's documentation consists of an overarching CSA supported by four annexes:

- Site and Plant Information (including categorisation of materials for protection against theft),
- Identification of Candidate VAs and CBSIS,
- Application of NIMCA, and
- Security Infrastructure

33. The annexes are supported by a number of appendices. In total there are 25 documents. There is a large amount of information in the document, which has been structured in such a way as to enable each of the appendices to be used as standalone documents. The document contains information of varying classification ranging from commercially sensitive to SECRET Sensitive Nuclear Information (SNI) and has been formatted and arranged to separate lower classification information from higher classification information. Hitachi-GE has incorporated a fifth annex (Compliance Document) which details their own undertaking to demonstrate compliance with GDA security requirements and NORMS.

34. For security, the following sections of the CSA have been central to the assessment:

- categorisation of materials for protection against theft,
- Vital Area (VA) identification,
- identification of CBSIS and OT
- identification of Computer Systems Important to Security (CSISy)
- concept of security operations
- power to the security infrastructure

35. Key sections of the document that I have assessed have been:

- **Annex A (Appendices A.1 – A.4) - Site and Plant Information**. Hitachi-GE has provided a description of the main UK ABWR buildings together with a table summarising the characteristics of the UK ABWR civil structures within the scope of GDA. Hitachi-GE has also summarised the fundamental safety functions and their associated SSCs, operating state and description of fuel route operations. Importantly, Hitachi-GE has provided details of NM/ORM inventories and categorised the material for theft based on the NORMS categorisation tables. As a result of this process, Hitachi-GE has placed the facility into an appropriate category for theft. This annex also includes the location of doors and evacuation routes.

- **Annex B (Appendices B.1 – B.5)** – **Identification of Critical Assets, C&I, CBSIS and OT**. The annex details the methodology used in order to identify

the candidate Critical Assets as part of the VA identification process. This methodology allowed Japanese SME's to be involved in the process and to provide input to the selection of the candidate Critical Assets. Each candidate Critical Asset which alone or in combination could give rise to a URC when challenged using the NIMCA threats has been confirmed as a Critical Asset and taken forward in the process. In terms of CBSIS and C&I, Hitachi-GE has used safety categorisation to determine those systems that could be termed Critical Assets. Hitachi-GE has also described how the potential for cyber threats has been examined and the mitigations in place to protect against a URC from a cyber-attack.

- **Annex C (Appendices C.1 – C.5) – Application of a UK DBT**. Using UK nationals, Hitachi-GE has applied the NIMCA to further progress its VA identification work. Hitachi-GE has also expanded on the cyber threats to determine critical Operational Technology (OT) which require protection. Analysis has also been undertaken by Hitachi-GE to determine the effects of blast on systems, structures and components as well as conduct adversarial pathway assessments. The pathway assessments determine potential routes an adversary may take to SSCs and assist with identifying the most effective strategy for applying the physical security infrastructure.

- **Annex D (Appendices D.1 – D.5) – Security Infrastructure**. Subsequent to identifying those assets requiring protection, Hitachi - GE has documented the security infrastructure which is intended to protect those assets identified. The security infrastructure provides detail of access control arrangements, considers physical security measures and their power supply and outlines a concept of security operations.

36. I have not assessed Annex E, Hitachi-GE's Compliance Document. While I consider an internal review/assurance exercise good practice to underpin Hitachi-GE's own confidence in their submission, my judgements are based purely on those areas related to the security arrangements documented in the CSA.

37. The following documents constitute Hitachi-GE's submissions which make up the CSA:

UKABWR Conceptual Security Arrangements	Overarching Document Ref: GA91-9101-0301-00001
Annex A	Site & Plant Information
Appendix A.1	General Plant Information
Appendix A.2	Site and Building layout Drawings
Appendix A.3	NM/ORM Inventory and Categorisation
Appendix A.4	Location of doors and evacuation routes
Annex B	Identification of Candidate Critical Assets, C&I and CBSIS
Appendix B.1	Identification of CAs
Appendix B.2	List and Locations of CAs
Appendix B.3	E,C&I and CBSIS
Appendix B.4	List and locations of C&I and CBSIS
Appendix B.5	Location of Power Supply to Candidate CAs
Annex C	Application of NIMCA Threats to identify Vital Areas

Appendix C.1	Physical Design Basis Threat
Appendix C.2	Cyber Design Basis Threat
Appendix C.3	Pathway Assessments
Appendix C.4	Blast Modelling
Appendix C.5	Location and Security Classification of UK ABWR VAs
Annex D	Security Infrastructure
Appendix D.1	Access Control Arrangements
Appendix D.2	List of CSISy and PSM
Appendix D.3	Power Supply to the Security Infrastructure
Appendix D.4	Concept of Operations
Appendix D.5	UK ABWR IPS Structure
Annex E	Compliance Document

4 ONR STEP 4 ASSESSMENT

38. This assessment has been carried out in accordance with ONR internal guidance 'Guidance on the Security Assessment of Generic New Nuclear Reactor Designs '

4.1 Scope of Assessment Undertaken

39. The overall aim of the assessment of the CSA is to judge whether Hitachi-GE has developed adequate conceptual security arrangements for the UKABWR that can be incorporated into the licensee's site specific security plan. Site specific arrangements, such as perimeter fences, site access control, ongoing personnel security, security force locations and security response are outside the scope of this assessment and remain the responsibility of the licensee to develop. However, it is acknowledged that these arrangements play a vital role in providing defence-in-depth, especially in mitigating external threats.

40. The extent of these arrangements to be developed by the licensee may influence those conceptual arrangements put forward by the RP when the licensee comes to develop the site specific security plan. However, my assessment takes into account all threats described in the extant NIMCA including those posed by insiders, which provide unique challenges due to the advantages of having authorised access and by their very nature, the ability to circumvent some site specific arrangements. In this respect, my assessment primarily focussed on physical measures controlling access to sensitive areas and did not examine those important measures such as vetting, security culture and aftercare which will be for the licensee to develop.

41. For computer systems, the scope of the assessment considered computerised safety systems in the context of preventing (Unacceptable) Radiological Consequences (URC). Computerised safety related systems have been considered in a proportionate manner, reflecting the consequences of compromise and recognising the opportunities for individual site specific choices to be made regarding these systems. This has been assessed separately by CS&IA inspectors and included separately as an annex to this report available to Hitachi-GE.

42. At some sites, including nuclear power stations, an act of sabotage involving NM/ORM, or against specific equipment, systems or devices comprising part of the site's infrastructure could create a radiological hazard to the public and/or the environment. At such sites, the potential for sabotage and the associated potential radiological consequences are evaluated. The purpose of the evaluation is to identify key assets associated with unacceptable radiological consequences so they can be designated as a VA and protected by appropriate security measures using a graded approach. This has been assessed separately by SINS inspectors and included separately as an annex to this report.

4.2 Categorisation of Materials for Protection Against Theft

43. In order to apply a proportionate level of protection against theft, NORMS requires the total amount of NM on site, or in a group of buildings, to be added together to determine the categorisation of the site or group of buildings as a whole.

44. Within Appendix A.3 of the CSA, Hitachi-GE has provided an inventory of nuclear material (NM) and other radioactive material (ORM) including radioactive wastes. This inventory has been based on the UK ABWR March 2016 Design Reference. The listed inventory includes a description of the material, its location, quantity, form and characteristics.

45. Hitachi-GE has conducted analysis of the inventory against the NORMS categorisation Tables 1[3] and 2[4] and determined the highest category of the facility during its lifetime. This is based on the use of <5% enriched uranium and classification of irradiated material as defined in the Table 1.

46. I am satisfied that Hitachi-GE has adequately categorised the UKABWR against theft for physical protection purposes in order to determine and apply appropriate and proportionate conceptual security arrangements for the protection of the material. My judgement is based on the detailed list of NM and ORM inventory which Hitachi-GE has detailed in Appendix A.3 and the use of and comparison against the NORMS categorisation table. In addition, the level of enrichment of fuel to be used in the reactor is similar to that used in existing operating reactors in the UK.

4.3 The Graded Approach to the Protection of Vital Areas Against Sabotage

47. The UK ABWR CSA presents Hitachi-GE's methodology for determining VAs in the design. Hitachi-GE's submission considers the threats presented in the extant NIMCA against NM and ORM, and the systems, structures and components of the UK ABWR GDA design. The support of UK contractors has allowed the security issues associated with the contents of the NIMCA to be addressed and this in turn has provided for a comprehensive Vital Area identification which has taken account of the UK's Design Basis Threat (DBT) as defined in the extant NIMCA document.

48. Within the CSA, the Vital Area Identification study has been undertaken in line with the project methodology that ONR has previously accepted in Step 2. A blast assessment is presented as part of the Vital Area Identification in order to determine the vulnerability of structures and systems. The detailed findings of the Vital Area Identification process are presented within the CSA and have been used to inform the conceptual security arrangements.

49. The assessment of the Vital Area identification work as presented in the CSA has been undertaken by ONR Security Informed Nuclear Safety (SINS) Inspectors. ONR Technical Assessment Guide CNS-TAST-GD-6.2 – Target Identification for Sabotage has been used to judge the adequacy of this section of the CSA. A summary of the assessment in this area is documented in Annex 1. The assessment concluded that the Vital Area Identification study is based on appropriately conservative assumptions considering the whole range of NIMCA threats and is considered adequate.

50. Some VA information presented in Appendix C5 is not consistent with that given in the high level CSA document for VAs. The CSA document shows "Potential Vital Area 2" areas in locations where the plant design is yet to be confirmed as part of the site specific phase of the design. The potential VA 2 areas are not listed in the key for the VA layouts in Appendix C5. However they appear to be shown on the drawings which could be taken as indicating they are confirmed VAs. This will require clarification by the licensee as part of the site specific security plan development.

51. One assessment finding relating to the VA identification process was identified:

AF-ABWR-SEC-01: Modifications to plant design will require a re-evaluation of the VA status. Late design changes to some areas of the plant have been taken into account by Hitachi-GE and a conservative re-evaluation undertaken which has identified *potential* VAs. In addition, some VAs were identified using generic data, and conservative assumptions made. These VAs should be re-evaluated using site

[3] *NORMS Table 1 – Categorisation of Nuclear Material*
[4] *NORMS Table 2 – Intermediate or Low level Wastes Containing Nuclear Material*

specific data to confirm or otherwise VA status. The identified anomalies relating to the VAs in the CSA appendices should be reviewed and corrected.

4.4 Computer Based Systems Important to Safety and Operational Technology

52. In Appendix B.3, Section 2, Hitachi-GE has described three C&I systems by which they achieve independent and diverse defence in depth. These systems are the Plant Control System (PCntlS), the Safety System and Logic Controller (SSLC) and the Hard Wired Back-up System (HWBS). By adopting this architecture, should the PCntlS or SSLC be compromised by cyber means, the HWBS would be the third independent and diverse line of defence to protect against a URC. This is supported by Hitachi-GE fault studies and the HWBS being non-computerised and invulnerable to attack by cyber means alone.

53. All systems identified as CBSIS and the HWBS have been designated as Critical Assets (CA) by Hitachi-GE. CAs are subject to specific physical security arrangements as detailed in in the CSA.

54. Hitachi-GE has adequately demonstrated for GDA that they can prevent a URC initiated through cyber means alone. They have achieved this by placing a non-computerised, independent and diverse system (HWBS) in the safety sequence thereby eliminating the cyber risk in regard to a URC. Defence in depth is reinforced by the application of cyber security to the PCntlS and to an even higher degree the SSLC.

55. Whilst there is sufficient evidence to conclude the cyber security is adequate for the purpose of GDA in preventing a URC, NORMS places a greater onus on licensees to demonstrate that CBSIS are adequately protected against cyber-attack, manipulation, falsification and sabotage. The scope of Section 4 of Appendix B.3 is clear that an event less than a URC is excluded, which for GDA is considered to be proportionate. However, a licensee will still need demonstrate that CBSIS are adequately protected against cyber-attack, not only for URC but also for lower consequences.

AF-ABWR-SEC-02: The cyber analysis undertaken by Hitachi-GE used a combination of deterministic and probabilistic analyses based on the most capable of threat actors, which was considered adequate for GDA as it supports the evidence related to the overall architecture of the safety systems. A broader risk assessment covering the full range of threat actor capability will need to be adopted by the licensee once site specific technology has been chosen and when developing the site security plan.

4.5 Threat from Insiders

56. Effective mitigation against insider threats requires the identification of those areas which are vulnerable to malicious acts carried out by insiders and the application of both physical measures and procedural controls to mitigate this threat. The latter should be developed by the licensee; however, it is important that appropriate physical security arrangements are in place to support the procedures adopted by the licensee.

57. Hitachi-GE has used a methodology accepted during earlier stages of GDA to identify critical assets and vital areas (VAs). The concept of security operations described in the CSA effectively applies a proportionate physical protection system (PPS) across the plant whereby those areas considered to have potentially the highest consequences have the most stringent level of physical security.

58. Hitachi-GE has identified and categorised VAs and applied a range of security measures which provide deter, detect and delay functions to enable effective

response. As well as detailing the access controls placed on these areas Hitachi-GE has also identified the requirement for implementation of a 'two person rule' in the most sensitive areas.

59. The development of the arrangements align with relevant good practice for Insider Risk Assessment provided by CPNI in that Hitachi-GE has:

- Identified the critical assets in the plant,
- Applied a Design Basis Threat (NIMCA),
- Assessed the impact of the threat
- Proposed proportionate measures to reduce security risks.

I am satisfied that, within the scope of GDA, Hitachi-GE has developed adequate conceptual security arrangements which will allow the licensee to integrate these arrangements with the essential procedural measures to provide effective mitigation against insider threats.

4.6 Vulnerability Assessment

60. NORMS identifies the requirement for vulnerability assessments. The scope of such assessments within GDA is limited as all aspects of a facility's security infrastructure should be taken into account including those measures outside of the GDA scope such as response force and perimeter protection.

61. Hitachi-GE has followed the methodology described in NORMS in that they have identified potential sabotage targets, confirmed applicable NIMCA threats and produced likely adversarial scenarios and pathways for sabotage. They have used this methodology to determine appropriate physical security measures to be adopted to address the potential vulnerabilities.

62. I consider that the adversarial pathway analysis has proved useful in identifying potential routes to VAs that could be exploited to give the most direct access to targets. This has allowed Hitachi-GE to apply proportionate security measures (detection, delay and assessment) at key points in the design. It should be noted that this vulnerability analysis has been conducted using a conservative approach which has excluded site specific security measures such as perimeter fences, barriers and security response which were outside the scope of this GDA.

4.7 Building Resilience

63. Hitachi-GE has examined NIMCA-based threat scenarios and in doing so, has assessed the standards of building structures to withstand relevant threats. The external blast assessments undertaken by Hitachi-GE analyse the response of specific UK ABWR structural elements subjected to a range of attack scenarios in order to determine stand-off distances that will ensure nuclear safety is not challenged. The stand-off distances so derived will be used to establish the security requirements that the licensee will need to develop as part of the site specific arrangements. Assessment undertaken by ONR safety inspectors concluded that Hitachi-GE adopted a conservative and appropriate approach to address this topic and concluded that appropriate standoff distances have been calculated.

4.8 Security Architecture

64. The overarching principle applied to UK ABWR security measures is to prevent unauthorised access. This has been demonstrated in the UK ABWR design by adopting a defence-in depth approach in which a series of barriers and access controls

ensures that only those personnel with appropriate authorisation and a "need to go" gain access.

65. Hitachi-GE has taken account of plant operating states and the differing access requirements from normal operating state through to major outage. Through all operating states the physical security measures put in place should ensure access to individual rooms or areas is restricted to authorised persons. In practice this means an authorised individual accessing any one of the buildings in the nuclear island does not necessarily have automatic access to a particular area or room within that building or to another building. This has the potential to limit the activity of an insider and prevent the freedom of movement of intruders.

66. Hitachi-GE has developed a range of controls to deliver detection, delay and assessment to allow for an appropriate and timely response to any attempted unauthorised access or activity. These measures include the following and are deployed in a proportionate manner to protect defined areas:

- Two-person unlock procedure[5] + remote verification[6] + CCTV + Alarm
- Dual verification[7] + CCTV + alarm
- Radiologically Controlled Area (RCA) Authorisation + Dual Verification
- Dual verification

67. In appendix D.2 of the CSA Hitachi-GE has provided a high level description of the Security Management System which encompasses those systems that fall into the category of CSISy as defined in NORMS. These systems, which provide the functions of detection, delay and assessment, and facilitate appropriate response, have been listed in the CSA, each with a set of attributes and general requirements that should be considered during site specific development. Hitachi-GE has also provided high level detail of the potential consequences of loss of these systems and expected measures to protect these systems from threats.

68. I consider that Hitachi-GE has provided an adequate high level concept of the security systems for the GDA. Technology in this area is progressing rapidly and it will be for the licensee to develop arrangements to support its security infrastructure and concept of security operations. As the majority of these systems will be computer based, it is important that the licensee carries out a cyber risk assessment of the CSISy.

69. Site specific operating procedures and instructions are outside the scope of the assessment and are the responsibility of the licensee. I consider the proposed physical security measures to be incorporated into the nuclear island will provide effective mitigation of threats if properly integrated with effective site wide security arrangements such as PIDS, barriers, procedures, instructions and response to provide overall defence in depth.

70. Hitachi-GE has adopted a graded approach to protecting identified assets. In relation to forcible attack, Hitachi-GE has used CPNI Protection Levels – Base, Enhanced and High to define the standard required for each door on the nuclear island. This is supplemented by the CPNI Class ratings for protection against surreptitious attack. It will be for the licensee to ensure that site specific equipment meets those standards. I consider that the adoption of CPNI standards by Hitachi-GE is good practice and provides a strong basis for the licensee to develop site specific arrangements.

4.9 Provision of Back-up Power to the Security Infrastructure

[5] *Procedure requires the attendance of two authroised persons to gain access*
[6] *Remote verification should be carried out from a security control room*
[7] *Dual verification should be a combination of two qualifiers which can include passes, PIN or biometric information.*

71. Hitachi-GE has provided high level detail on the means to provide power to the security systems in the event of loss of off-site power (LOOP). An estimate of the power requirements for the security infrastructure within the scope of GDA has been provided. This was considered to be the upper bounds of the power requirements by Hitachi-GE but does not extend to the site specific aspects of the security infrastructure such as perimeter lighting, site-wide CCTV, Perimeter Intruder Detection (PIDs). Such infrastructure may result in greater power requirements and will need to be taken into account by the licensee in designing site specific arrangements.

72. Hitachi-GE has stated that an Uninterruptable Power Supply (UPS) provides power to security systems in the event of LOOP or faults on the plant power distribution system. Hitachi-GE has not identified a specific back-up generator solution for the security infrastructure which will be required in the event of a loss of supply and have acknowledged the risk that the Emergency Diesel Generators (EDG's) and Diverse Alternate Generator (DAG) may not have spare capacity. Claims made on the use of the EDG's and DAG cannot be substantiated in GDA.

73. The source of back-up power to the security systems has been discussed with the inspector assessing electrical power and it was agreed that it has not been adequately defined. The options for allocating power capacity from EDGs/DAG or the provision of alternative standby AC power sources have not been determined and no definitive provision for supplies to security systems have been provided in the design of the electrical system. The design of the power distribution to the security systems to take account of the need to minimise the risk of common cause failure has not been addressed. Hitachi-GE has claimed that battery UPS will be located with the equipment they support within protected areas. Hitachi-GE has argued that this co-location provides equal levels of protection to the UPS.

74. In terms of the UPS, I am content that the proposed arrangements protecting those critical assets also provide a bounding case for the protection of the UPS to those systems within the scope of GDA.

75. In the scope of GDA and in terms of meeting NORMS, I am satisfied that Hitachi-GE has, at a high level, considered the requirement for UPS and backup power for the security infrastructure. However, later design changes in the plant design prevented the CSA from making a reliable claim that the EDGs and DAG would provide power to security systems in an emergency. It will now be for the licensee to design the power supply to the security systems to minimise the risk of power failure to the security systems and document this in the specific site security plan.

AF-ABWR-SEC-03 The licensee shall identify the requirement for, and provision of power to the site security systems in order to minimise the risk of power failure.

4.10 Safety/Security Interface

76. NORMS requires that, during the design phase of a new project, any conflicting safety and security requirements should be identified as early as possible. An effective change control mechanism must be utilised to ensure any proposed changes to design, layout or procedures are evaluated to assess the potential impact on security.

77. Hitachi-GE document 'Implementation procedure for GDA Design Change Process'[8] details the process for implementing design changes and includes a means of determining the impact a potential design change has on any other particular topic area. It is important that security requirements are taken into account when design changes are being considered and any potential impact on security is addressed.

[8] *Hitachi-GE – GA10-0002-00001 – XD-GD-0005*

78. Hitachi-GE has ensured that access to identified VAs remain controlled at all times including during emergency evacuation. This has been achieved by re-routing or reconfiguring evacuation routes to ensure that there are no areas of uncontrolled access from lower level security zones into or through a higher level security zone. Hitachi-GE has confirmed this does not impact on conventional fire safety requirements.

4.11 Assessment findings

79. Assessment Findings are residual matters that must be addressed by the licensee and the progress monitored by the regulator.

80. During my assessment, three assessment findings were identified for a future licensee to take forward in their site-specific security submissions. Details of these are contained in Annex 5.

81. These findings do not undermine the generic security submission and are primarily concerned with the provision of site specific security case evidence, which should become available as the project progresses through the detailed design, construction and commissioning stages.

82. I have recorded residual matters as assessment findings if one or more of the following apply:

- site specific information is required to resolve this matter;
- resolving this matter depends on licensee design choices;
- the matter raised is related to operator specific features / aspects / choices;
- the resolution of this matter requires licensee choices on organisational matters; and
- to resolve this matter the plant needs to be at some stage of construction / commissioning.

5 CONCLUSIONS

83. This report presents the findings of my Step 4 security assessment of the Hitachi-GE UK ABWR.

84. To conclude, I am satisfied with the claims, arguments and evidence laid down within the CSA. I consider that from a security view point, the Hitachi-GE UK ABWR design is suitable for construction in the UK subject to future development and approval of site specific security arrangements.

85. Three assessment findings (Annex 5) were identified; these are for the future licensee to consider and take forward in their nuclear site security plan. These findings do not undermine the generic security submission but will require licensee input/decision.

6 REFERENCES

1 UK ABWR Conceptual Security Arrangements Document - GA91-9101-0301-00001 dated 21 August 2017

2 ONR's GDA Guidance to Requesting Parties
http://www.onr.org.uk/new-reactors/ngn03.pdf

3 National Objectives, Requirements and Model Standards (NORMS) for the Protective Security of Civil Licensed Nuclear Sites, Other Nuclear Premises and Nuclear Material in Transit - Issue 2

4 Nuclear Industries Malicious Capabilities Planning Assumptions

5 Classification Policy for the Civil Nuclear Industry – Information concerning the use, transport and storage of Nuclear Material and Other Radioactive Material.
http://www.onr.org.uk/documents/classification-policy.pdf

6 UK ABWR Step 4 Assessment Plan for Security – ONR-GDA-AP-15-014

7 IAEA Nuclear Security Recommendations on Physical Protection of Nuclear Material and Facilities (INFCIRC/225/Revision 5)

8 IAEA Convention on the Physical Protection of Nuclear Material

9 ONR Security Assessment Principles (SyAPs) 2017 Edition, Version 0
http://www.onr.org.uk/syaps/security-assessment-principles-2017.pdf

10 ONR SINS Assessment of the Vital Area Identification provided within the UK ABWR Conceptual Security Arrangements document – ONR-CNS-AR-17-028

11 Assessment of Cyber Security & Information Assurance for the UK ABWR – ONR-NR-AN-17-004

12 Anti-terrorism, Crime and Security Act 2001

ANNEX 2

Security of Computer Based Systems Important to Safety and Operational Technology

Documents assessment based on

1. The Hitachi-GE security case for Cyber Security & Information Assurance for CBSIS is contained within UK ABWR GDA, Conceptual Security Arrangements Appendix B.3 – E, C&I and CBSIS. Document reference GA91-9101-0301-00001 (App.B.3). Appendix B.3 is 170 pages. Linked to this is Appendix C.2 Cyber Design Basis Threat. Document reference GA91-9101-0301-0001 (App. C.2). Appendix C.2 is 24 pages.

2. Appendix B.3 section 1 is the introduction and sets out a few key concepts. The main one being that both CBSIS and hardwired C&I systems have been considered Critical Assets (CA) and will have physical security arrangements as set out across the CSA. The introduction also sets out some key assumptions that the Appendix relies upon.

3. Section 2 defines the key components of the UK-ABWR C&I safety systems. These are the Safety System Logic and Control (SSLC) system, the Plant Control System (PCntlS) and the Hard Wired Back-up System (HWBS). The section goes on to cover the methodology for the identification of CBSIS and describes the high level relationship between the three main systems. For the identification of CBSIS the Design Basis Analysis (Doc ref GA91-9201-0001-00023 Rev 13) and Topic Report on Fault Assessment (Doc ref GA91-9201-0001-00022 Rev 6), colloquially referred to as fault study reports in this appendix, contain the methodology used to identify CBSIS. The overall safety systems architecture is predicated on achieving the prevention of an event that would result in an Unacceptable Radiological Consequence (URC). Where an event does take place the hierarchical systems can independently take control from the lower system to take the plant to a safe state.

4. The section continues to examine the three major systems in relation to the fault studies. Hitachi-GE state that the complete and simultaneous loss of both the PCntlS and SSLC by any cyber and/or physical means will not result in a URC. To achieve a URC would require a physical attack on the HWBS in addition to the simultaneous attacks on both the PCntlS and SSLC. In order to maintain the defence in depth all three systems are classified as CAs. The HWBS is explained and a high degree of confidence is expressed that it will be free from computerised technology making it invulnerable to cyber-attack. The HWBS is examined in more detail in the Topic Report on Hardwired Back-up System Platform (Doc ref GA91-9201-0001-00153 Rev 1).

5. Section 3 looks at the high level integration of physical, personnel and cyber security. It also introduces the Hitachi-GE GDA Cyber Design Based Threat (DBT).

6. Section 4 identifies the scope of GDA in respect of cyber security of C&I and the use of the cyber DBT. The scope of the cyber DBT is limited to design activities of the ABWR C&I systems. The cyber DBT is only applied if a URC is considered a possibility. Loss of generation, plant damage, reputational damage or theft of SNI/Nuclear Material is not specifically assessed as potential consequences of an attack by capabilities described in the cyber DBT. Any future licensee would need to develop its own cyber DBT accounting for site specific threats and these other types of consequence. The Hitachi-GE analysis of the potential consequences of an attack by those capabilities indicates that a cyber-attack would need to be supported by a physical attack on the HWBS to achieve a URC.

7. In section 5 it is confirmed that an assessment based on HMG Information Assurance Standard No1 has not been adopted in favour of a Probabilistic Risk Assessment (PRA) approach. The PRA initially considers the PCntlS and through Hitachi-GE's own conservative calculations identifies a frequency of successful cyber-attacks on the PCntlS over the 240 reactor years for the ABWR. Whilst the frequency of a successful cyber-attack is identified, the consequence of the cyber-attack is that the PCntlS does not operate as intended and does not result in a URC. The PRA then factors in the likelihood of successful attack on both the SSLC and the HWBS, which in combination could result in a URC. These calculations are based on a Hitachi-GE conservative methodology. In the PRA, the attack against the SSLC and HWBS is not limited to a cyber-attack because physical attack will be required in in combination to a cyber-attack to potentially result in a URC. A gap analysis of the contents of NORMS 1.1.89 to 1.1.95 is undertaken in this section. In this gap analysis there are two key points. As well as being classified as CAs the systems are also considered 'in combination Vital Areas (VAs)' and will be located in highly secure building zones. The gap analysis also concludes that for the development of an NSSP a broader risk based approach similar to IS1 will be required.

8. Section 6 considers the potential of an insider attack and the controls to mitigate this threat.

9. Section 7 describes the configuration management, quality assurance, validation & verification and testing of the systems during design and development.

10. Section 8 provides an overview of the design features of the UK-ABWR C&I systems and how their design, redundancy, diversity and technology choices support cyber security. The three main systems (PCntlS, SSLC and HWBS) are reviewed in more depth. The architecture, technology, location, power supply and environmental controls are detailed in this review along with a number of other items. Network isolation is considered in consideration of a Stuxnet type attack.

11. Section 9 provides a compliance statement against both the Civil Nuclear Security Cyber Security Strategy (Ref. 8) and IEC 62645 (Ref. 9).

12. Sections 10-14 consider a number of areas associated with the security of CBSIS. These are; threats during manufacture and transit, threats during construction and commission, threats during operation and maintenance, control room security, malicious electromagnetic waves and electromagnetic pulse to attack CBSIS.

13. Section 15 is the compliance matrices of Hitachi-GE against IEC 62645 and relates to section 9.

The Cyber Design Based Threat

14. The objective of Appendix C.2, Cyber Design Basis Threat (DBT) is to define and describe the DBT in relation to the UK ABWR GDA project. The boundaries of the cyber DBT are the maximum credible threats from the most capable threat that could lead to a URC. It does not consider lower consequences. The GDA project is defined in the cyber DBT as design, construction, commissioning and handover of plant to the licensee. The NIMCA is analysed for structure and a GDA specific cyber DBT is produced that considers group size, equipment, capabilities, tactics, methodologies and state responsibilities.

Scope of Assessment Undertaken

15. Having reviewed Hitachi-GE's submission, the scope of the assessment mainly focussed on 1.1.90 of NORMS, recreated here:

> Dutyholders are to identify and categorise CBSIS, in order that a graded approach to security can be applied to these systems. A CBSIS is a system that falls into one or both of the following categories:
>
> a) Safety systems: computer systems that are part of a nuclear safety system, i.e. systems that respond to a potentially hazardous plant fault by implementing the safety action necessary to prevent radiological consequences; and
>
> b) Safety-related systems: any other computer systems that could through their actions or lack thereof, have an adverse effect on the safety of a nuclear system (e.g. a control system that maintains working parameters within pre-defined limits by responding continuously to normal plant operations).

16. The scope of the assessment considered computerised safety systems in the context of preventing (Unacceptable) Radiological Consequences (URC) as contained in NORMS 1.1.90 a) above. Computerised safety related systems, 1.1.90 b) above, have been considered in a proportional manner, reflecting the consequences of compromise and the opportunities for individual site specific choices to be made regarding these systems.

17. The identification and categorisation of CBSIS is a specialist safety activity where a clear understanding of the safety function delivered by each system must be understood and an informed assessment of the Hitachi-GE approach can be made. This will also allow for a graded approach to be applied to each system ensuring the appropriate level of protection is put in place. This area has been integrated with the C&I topic area.

Assessment

18. In Appendix B.3, Section 2, Hitachi-GE has described three C&I systems by which they achieve independent and diverse defence in depth. These systems are the PCntlS, the SSLC and the HWBS. By adopting this architecture, should the PCntlS or SSLC be compromised by cyber means, the HWBS would be the third independent and diverse line of defence to protect against a URC. This is supported by Hitachi-GE fault studies and because the HWBS is a system that we have a high degree of confidence is free from computerised technology, and thus invulnerable to attack by cyber means alone. *This is backed up by the C&I inspectors' review of the independence, segregation and diversity claimed for HWBS, detailed in RO-ABWR-0027.* In RO-ABWR-0027 C&I inspectors review the independence, segregation and diversity claimed for HWBS.

19. The technology used in the HWBS does not include microprocessors or programmable complex electronic components. This eliminates the cyber threat to this system. The technology used in the SSLC is Field Programmable Gate Array (FPGA) which, in comparison to a microprocessor, is a less flexible technology (i.e. the skills, personnel and processes needed to change the function of an FPGA are significant) and therefore less susceptible to cyber-attack. The use of FPGA is more likely to require the development of system specific code in order to carry out any sort of cyber-attack on the SSLC.

20. In the introduction and in section 8 of Appendix B.3 all systems identified as CBSIS have also been designated as Critical Assets (CA) by Hitachi-GE. CAs are subject to specific physical security arrangements as detailed across the Conceptual Security Arrangements (CSA) documents. It also clarifies that the HWBS is also a CA. The adequacy of the physical security arrangements of CAs is covered elsewhere in this report.

21. From section 6 onwards of Appendix B.3 Hitachi-GE identify steps by which they can reduce the likelihood of cyber compromise of the SSLC. These steps are considered good practice within the scope of the bounding case made within Appendix C.2, cyber DBT. Hitachi-GE apply good practice to reduce the likelihood of cyber compromise of the SSLC, this is implemented despite Hitachi-GE evidence that a simultaneous compromise of both the PCntlS and SSLC by cyber means would not result in a URC.

22. NORMS details that a complex CBSIS will be inspected against the Risk Assessment Method detailed in HMG Information Assurance Standard No. 1 (IS1) or similar suitable methodology. Within section 5 of Appendix B.3 Hitachi-GE, in UK terms, adopt a novel Probabilistic Risk Assessment (PRA) approach in which they are able to conclude the probable frequency of a successful attack. The PRA approach is considered adequate for this GDA assessment as it supports the evidence relating to the overall architecture of the safety systems and the resistance to URC. Hitachi-GE goes on to acknowledge the effectiveness of PRA may be limited to GDA and that licensees may need a broader risk based approach to satisfy regulatory approval of an NSSP. This is a position, in relation to a broader risk based approach for the licensee, which I support.

23. In summary Hitachi-GE have adequately demonstrated for GDA that that they can prevent a URC conducted through cyber means alone. They have achieved this by placing a system, the HWBS, that we have a high degree of confidence is free from computerised technology, is independent and diverse in the safety sequence, thereby eliminating the cyber risk in regards of a URC. In order to maintain defence in depth, cyber security of the PCntlS and to an even higher degree the cyber security of the SSLC has also been considered in Appendix B.3.

24. Whilst there is enough evidence to conclude the cyber security is adequate for the purpose of GDA in preventing a URC, NORMS places greater onus on licensees to demonstrate that CBSIS are adequately protected against cyber-attack, manipulation, falsification and sabotage. Section 4 of Appendix B.3 is clear that an event less than a URC is not assessed, which for GDA may be proportionate. However a licensee will need demonstrate that CBSIS are adequately protected against cyber-attack, not only for URC but proportionately for lower consequences, this has not been demonstrated in GDA. I agree with the position expressed by Hitachi-GE's that the effectiveness of PRA may be limited to GDA and that licensees may need a broader risk based approach to satisfy regulatory approval of an NSSP. Limiting the scope of the cyber DBT to design activities also demonstrates the need for the licensee to undertake site specific work in this area. For these limitations within GDA I am making a single Assessment Finding.

25. The licensee must implement a suitable CBSIS cyber security risk assessment methodology and supporting management system that aligns with appropriate standard to manage the risks identified in these systems.

CONCLUSIONS

26. This note presents the findings of my Step 4 Cyber Security and Information Assurance assessment of the Hitachi-GE UK ABWR.

27. To conclude, I am broadly satisfied with the CSA and supporting documentation for the Cyber Security and Information Assurance specialism. I consider that from a Cyber Security and Information Assurance view point, the Hitachi-GE UK ABWR design is suitable for construction in the UK subject to the licensee addressing the Assessment Finding, and future permissions & permits beings secured .

28. An assessment finding was identified; this is for future licensee to consider and take forward in their site-specific safety and security submissions. This matter does not undermine the generic safety and security submissions and requires licensee input/decision. The Assessment Finding is detailed below.

Assessment Finding

29. The cyber analysis undertaken by Hitachi-GE used a combination of deterministic and probabilistic analyses based on the most capable of threat actors, which was considered adequate for GDA as it supports the evidence related to the overall architecture of the safety systems. A broader risk assessment covering the full range of threat actor capability will need to be adopted by the licensee once site specific technology has been chosen and when developing the site security plan.

Key Findings from the Step 4 Assessment

30. I consider that from a Cyber Security and Information Assurance view point, the UK ABWR design is suitable for construction in the UK, at this present time, subject to the licensee addressing the Assessment Finding, and future permissions & permits beings secured.

Annex 3

Technical Assessment Guides

TAG Ref	TAG Title
CNS-TAST-GD-007	Guidance on the Security Assessment of Generic New Nuclear Reactor Designs
CNS-TAST-GD-6.2	Target Identification for Sabotage
CNS-TAST-GD-001	Guidance on the Purpose, Scope and Quality of a Nuclear Site Security Plan

Annex 4

National and International Standards and Guidance

National and International Standards and Guidance
Nuclear Industries Security Regulations (NISR 2003) as amended.
National Objectives, Requirements and Model Standards (NORMS) for the Protective Security of Civil Licensed Nuclear Sites, Other Nuclear Premises and Nuclear Material in Transit
INFCIRC/225/Rev 5 – IAEA Nuclear Security Series No.13. Nuclear Security Recommendations on Physical Protection of Nuclear Material & Facilities – January 2011
IAEA Nuclear Security Series No 4 - Engineering Safety Aspects of the Protection of Nuclear Power Plants against Sabotage Nuclear Security Recommendations on Physical Protection of Nuclear Material & Facilities – January 2011

Annex 5

Assessment Findings

Assessment Finding Number	Assessment Finding	Report Section Reference
AF-ABWR-SEC-01	Modifications to plant design will require a re-evaluation of the Vital Area status. Late design changes to some areas of the plant have been taken into account by Hitachi-GE and a conservative re-evaluation undertaken which has identified *potential* Vital Areas. In addition, some Vital Areas were identified using generic data, and conservative assumptions made. These Vital Areas should be re-evaluated using site specific data to confirm Vital Area status.	4.3 The graded approach to the protection of Vital Areas against sabotage.
AF-ABWR-SEC-02	The cyber analysis undertaken by Hitachi-GE used a combination of deterministic and probabilistic analyses based on the most capable of threat actors, which was considered adequate for GDA as it supports the evidence related to the overall architecture of the safety systems. A broader risk assessment covering the full range of threat actor capability will need to be adopted by the licensee once site specific technology has been chosen and when developing the site security plan.	4.4 Computer Based Systems Important to Safety and Operational Technology
AF-ABWR-SEC-03	Provision of Back-up power supply to security systems has not been determined by the RP. The licensee shall identify the requirement for, and provision of power to the site security systems in order to minimise the risk of power failure.	4.9 Provision of back-up power to the security infrastructure