New Reactor Division – Generic Design Assessment

Step 2 Assessment of the Security of UK HPR1000 Reactor

Assessment Report ONR-GDA-UKHPR1000-AR-18-006
Revision 0
October 2018

Published 10/18

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 results of my security assessment of the UK HPR1000, undertaken as part of Step 2 of the Office for Nuclear Regulation's (ONR) Generic Design Assessment (GDA).

The GDA process calls for a step-wise assessment of the Requesting Party's (RP) safety and security submissions, with the assessments increasing in detail as the project progresses. Step 2 of GDA is an overview of the acceptability, (in accordance with the regulatory regime of Great Britain), of the design fundamentals, including ONR's review of key nuclear safety and nuclear security claims (or assertions). The aim is to identify any fundamental safety or security shortfalls which could prevent ONR from permitting the construction of a power station based on the design.

During GDA Step 2, my work focused on the assessment of the Preliminary Safety Report (PSR) Chapter 27, as well as a number of supplementary documents submitted by the RP, focusing on design concepts and claims.

My GDA Step 2 assessment work involved regular engagement with the RP in the form of technical exchange workshops and progress meetings. Throughout GDA Step 2, I engaged with the RP regarding the protection of Sensitive Nuclear Information (SNI) to ensure they have the necessary security arrangements in place to comply with HMG's Security Policy Framework. To this end, the RP engaged both with me and specialist Personnel and Cyber Security and Information Assurance (CS&IA) inspectors, to ensure compliance with UK legislation and relevant good practice.

An important aspect of my work was the assessment of the RP's framework, allowing them to assess the Vital Area Identification (VAI) methodology using the UK Design Basis Threat (DBT), (known in the UK as the Nuclear Industries Malicious Capabilities (Planning) Assumptions (NIMCA)). The framework needs to allow for the fact that the NIMCA document bears a national caveat and cannot be released to non-UK citizens. In my opinion the RP has implemented an effective mechanism, using UK contractors, to allow this important work to be undertaken.

The standards I have used to judge the adequacy of the RP's submissions in the area of security have been primarily ONR's Security Assessment Principles (SyAPs) and ONR's Technical Assessment Guides (TAGs). I have also made use of other relevant standards and guidance.

The UK HPR1000 PSR is primarily based on the Reference Design, Fangchenggang Unit 3 (FCG 3), which is currently under construction in China. Key security aspects of the UK HPR1000 are presented in the PSR, and the supplementary documents submitted by the RP. These can be summarised as follows:

- The Security Case and its supporting annexes. This details the RP's objectives, claims and arguments.
- The Security Risk Management approach and its supporting annex.
- The VAI methodology, which includes the proposed Cyber Risk Assessment process.

During my GDA Step 2 assessment of the security arrangements for the UK HPR1000 I have identified the following areas of strength:

  - An adequate methodology to identify Vital Areas (VAs) has been prepared. This will allow the RP to focus the security arrangements on the areas of highest risk.
  - The RP has been proactive in determining a process by which the significant risks to the cyber security of the proposed design can be identified.

- The RP has demonstrated an adequate understanding of the basic security principles and how these can be applied throughout the GDA process.

During my GDA Step 2 assessment of the proposed security arrangements for the UK HPR1000 I have identified the following areas which will require further consideration by the RP during Step 3:

- The RP will need to develop clear arguments to support its claim of influencing the design following the VAI process and approach to Cyber Risks, and describe how this will be achieved.
- The RP has presented an holistic security picture which, in my opinion, will be of value to the organisation throughout the lifetime of the proposed reactor. During the future steps of the GDA, the RP will need to develop clear arguments about what is in the scope of the GDA, and how the claims detailed in Step 2 of the GDA, can be achieved.

During my GDA Step 2 assessment, I have not identified any fundamental shortfalls in the area of security which might prevent the issue of a Design Acceptance Confirmation (DAC) for the UK HPR1000 design.

LIST OF ABBREVIATIONS

ALARP	As Low As Reasonably Practicable
BMS	Business Management System
CCI	Commercially Confidential Information
C&I	Control and Instrumentation
CBSIS	Computer Based Systems Important to Safety
CBSyS	Computer Based Security Systems
CGN	China General Nuclear Power Corporation
CONOP	Concept of Operations
CS&IA	Cyber Security and Information Assurance
DAC	Design Acceptance Confirmation
DBT	Design Basis Threat
EA	Environment Agency
EDF	Électricité de France
FCG 3	Fangchenggang Nuclear Power Plant Unit 3
GDA	Generic Design Assessment
GNI	General Nuclear International
GNS	Generic Nuclear System Ltd
GSR	Generic Security Report
HMG	Her Majesties Government
IAEA	International Atomic Energy Agency
IEC	International Electrotechnical Commission
IT	Information Technology
JPO	(Regulators') Joint Programme Office
NIMCA	Nuclear Industries Malicious Capabilities (Planning) Assumptions
NM	Nuclear Material
NPP	Nuclear Power Plant
ONR	Office for Nuclear Regulation
ORM	Other Radioactive Material

OT	Operational Technology
PCSR	Pre-construction Safety Report
PSR	Preliminary Safety Report (includes security and environment)
RGP	Relevant Good Practice
RI	Regulatory Issue
RIA	Regulatory Issue Action
RO	Regulatory Observation
ROA	Regulatory Observation Action
RP	Requesting Party
RQ	Regulatory Query
SAP(s)	Safety Assessment Principle(s)
SFAIRP	So Far As Is Reasonably Practicable
SINS	Security Informed Nuclear Safety
SNI	Sensitive Nuclear Information
SQEP	Suitably Qualified and Experienced Person
SyAP(s)	Security Assessment Principle(s)
SyDP(s)	Security Delivery Principle(s)
TAG(s)	Technical Assessment Guide(s)
TSC	Technical Support Contractor
UK	United Kingdom
VA	Vital Area
VAI	Vital Area Identification

TABLE OF CONTENTS

1 INTRODUCTION 8
2 ASSESSMENT STRATEGY 9
2.1 Scope of the Step 2 Security Assessment 9
2.2 Standards and Criteria 9
2.3 Use of Technical Support Contractors 10
2.4 Integration with Other Assessment Topics 10
3 REQUESTING PARTY’S PROVISONAL SAFETY REPORT CHAPTER 27 AND SUPPORTING DOCUMENTS 11
3.1 The Security Case Report. 11
3.2 The Security Risk Management Approach 11
3.3 VAI Methodology 11
3.4 Cyber Security & Information Assurance (CS&IA) 11
3.5 Inventory of Nuclear Material (NM) and Other Radioactive Material (ORM) 12
3.6 Identified Operational Technology (OT) 12
3.7 Definitions, Abbreviations and Acronyms 12
3.8 Plant Information Record 12
4 ONR ASSESSMENT 13
4.1 The Security Case 14
4.2 Security Risk Management Approach 16
4.3 Vital Area Identification (VAI) methodology 17
4.4 Cyber Security & Information Assurance Assessment 18
4.5 Out of Scope Items 19
4.6 Comparison with Standards, Guidance and Relevant Good Practice 19
4.7 Interactions with Other Regulators 19
5 CONCLUSIONS AND RECOMMENDATIONS 20
5.1 Conclusions 20
5.2 Recommendations 20
6 REFERENCES 21

1 INTRODUCTION

1. The Office for Nuclear Regulation's (ONR) Generic Design Assessment (GDA) process calls for a step-wise assessment of the Requesting Party's (RP) submissions, with the assessments increasing in detail as the project progresses. General Nuclear System Ltd (GNS) has been established to act on behalf of the three joint RPs (China General Nuclear Power Corporation (CGN), Électricité de France (EDF) and General Nuclear International (GNI)) to implement the GDA of the UK HPR1000 reactor. For practical purposes, GNS is referred to as the 'UK HPR1000 GDA RP'.

2. During Step 1 of GDA, which is the preparatory part of the design assessment process, the RP established its project management and technical teams and made arrangements for the GDA of the UK HPR1000 reactor. Also, during Step 1 the RP prepared submissions to be assessed by ONR and the Environment Agency (EA) during Step 2.

3. Step 2 commenced in November 2017. Step 2 is an overview of the acceptability, (in accordance with the regulatory regime of Great Britain), of the design fundamentals, including ONR's assessment of key nuclear safety and nuclear security claims (or assertions). The aim is to identify any fundamental safety or security shortfalls which could prevent ONR permitting the construction of a power station based on the design.

4. My assessment has followed the GDA Step 2 Assessment Plan for Security (Ref. 1) prepared in October 2017 and shared with GNS to maximise openness and transparency.

5. This report presents the results of my assessment of the security arrangements for the UK HPR1000, as presented in the UK HPR1000 Preliminary Safety Report (PSR) Chapter 27 (Ref. 21) and supporting documentation (Refs. 2 - 12).

2 ASSESSMENT STRATEGY

6. This section presents my strategy for the GDA Step 2 assessment of the security aspects of the UK HPR1000. It includes the scope of the assessment and the standards and criteria applied.

2.1 Scope of the Step 2 Security Assessment

7. The objective of my GDA Step 2 assessment was to assess relevant design concepts and claims made by the RP related to security. In particular, my assessment has focussed on the following:

- The methodology to be adopted for the VAI
- The Cyber Risk Assessment process
- Security aspects of the reactor technology concept
- The SyAPs Fundamental Security Principles (FSyPs).

8. During GDA Step 2 I also evaluated whether the security claims are supported by a body of technical documentation sufficient to allow me to proceed with GDA work beyond Step 2.

9. Finally, during Step 2 I considered the following matters as part of my preparatory work for my Step 3 assessment:

- Development of the VAI process as it applies to the UK specific reactor design
- Development of the Cyber Risk Assessment process as it applies to the UK specific reactor design.

2.2 Standards and Criteria

10. For ONR, the primary goal of the GDA Step 2 assessment is to reach an independent and informed judgment on the adequacy of a preliminary nuclear safety and security case for the reactor technology being assessed. Assessment was undertaken in accordance with the requirements of the Office for Nuclear Regulation (ONR) HOW2 Business Management System (BMS) guide NS-PER-GD-014 (Ref. 13).

11. In addition, the ONR SyAPs (Ref. 14) constitute the regulatory principles against which the security of the RPs are judged and have been used in this assessment.

12. The relevant SyAPs and International Atomic Energy Agency (IAEA) standards are embodied and expanded on in the TAGs on security (Ref. 15). These guides provide the principal means for assessing the security aspects in practice.

2.2.1 Technical Assessment Guides

13. The following TAGs have been used as part of this assessment (Ref. 15):

- CNS-TAST-GD-6.1 (Rev 0) March 2020 Categorisation for Theft
- CNS-TAST-GD-6.2 (Rev 0) March 2020 Target Identification for Sabotage
- CNS-TAST-GD-6.3 (Rev 0) March 2020 Physical Protection System Design
- CNS-TAST-GD-7.3 Protection of Nuclear Technology and Operations
- CNS-TAST-GD-11.1 (Rev 0) June 2020 Guidance on the Security Assessment of Generic New Nuclear Reactor Designs

2.2.2 International Standards and Guidance

14. The following international standards and guidance have been considered as part of this assessment:

- Relevant IAEA guidance (Ref. 16)
  - IAEA Nuclear Security Series No.13 – Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilitates (INFCIRC/225/Revision 5).
  - IAEA Nuclear Security Series No.16 – Identification of Vital Areas at Nuclear Facilities
  - IAEA Nuclear Security Series No. 17 – Computer Security at Nuclear Facilities

- Relevant International Electrotechnical Commission (IEC) guidance (Ref. 17)
  - IEC 62645 Nuclear power plants - Instrumentation and control systems - Requirements for security programmes for computer-based systems
  - IEC 61226 Nuclear power plants. Instrumentation and control systems important to safety. Classification of instrumentation and control functions

2.3 Use of Technical Support Contractors

15. During Step 2 I did not engage a Technical Support Contractor (TSC) to support the assessment of the security for the UK HPR1000.

2.4 Integration with Other Assessment Topics

16. Early in GDA, I recognised the importance of working closely with other assessors (including Environment Agency's assessors), as part of the security assessment process. Similarly, other assessors sought input from my assessment of the security for the UK HPR1000. I consider these interactions key to the success of the project in order to prevent or mitigate any gaps, duplications or inconsistencies in ONR's assessment. From the start of the project, I endeavoured to identify potential interactions between the Security and other technical areas, with the understanding that this position will evolve throughout the UK HPR1000 GDA.

17. The identification of Computer Based Systems Important to Safety (CBSIS) and application of security measures has required close cooperation with Control and Instrumentation (C&I) assessors, particularly when defining CBSIS and assessing C&I architectures relevant to security.

3 REQUESTING PARTY'S PROVISONAL SAFETY REPORT CHAPTER 27 AND SUPPORTING DOCUMENTS

18. During Step 2 of GDA, the RP submitted Chapter 27 of the PSR, an outline of their proposed Generic Security Report (GSR) (Ref. 11) and a number of Tier 2 documents, which detail the proposed nuclear security arrangements for the UK HPR1000. This section presents a summary of the Tier 2 documents submitted for assessment during Step 2 of the GDA. These documents have formed the basis of my security assessment of the UK HPR1000 during GDA Step 2.

3.1 The Security Case Report.

19. This document aims to present the RP's security case in the form of a hierarchy of objectives, claims and arguments, which provides the framework in which the GNS VAI methodology and Cyber Risk Assessment methodology have been formulated and will be implemented. In Steps 3 and 4 of the GDA process this document will also provide the framework within which the security regime Concept of Operations (CONOP) will be developed. The Security Case is supported by Annex A: the Security Case Step 2 GSR Route Map and Annex B: the Security Case Claims and Arguments Table. (Refs. 2, 3 and 4)

3.2 The Security Risk Management Approach

20. This document aims to present the RP's security risk management approach, in the form of a security regime model, which the RP has utilised during the GDA process as the basis for formulating the VAI methodology. This document will also provide the framework within which the security regime CONOP will be developed. (Refs. 5 and 6).

3.3 VAI Methodology

21. The VAI Methodology documentation includes Cyber Risk Assessment and the associated VAI flow chart. (Ref. 7)

3.4 Cyber Security & Information Assurance (CS&IA)

22. The aspects covered by the GSR in the area of CS&IA are focused on CBSIS and are contained within the VAI Methodology, Annex B - Cyber Risk Assessment (Ref. 7). The annex identifies that CBSyS and IT will be assessed separately and, at enterprise level, it is assumed they will align with future relevant standards.

23. The annex describes a seven step process by which GNS will evidence that the generic design of the UK HPR1000 is secure by design and provides effective mitigation against the threats detailed in the NIMCA document. The process recognises there is a limitation on what can be incorporated into the 'secure by design' approach in GDA and that the future licensee will need to take responsibility for certain aspects of it, such as the security clearance levels of staff with access to the system.

24. The approach described is iterative and can be adapted to respond to changes in NIMCA, system classification or other changes.

25. The following steps are described in the document:

- Step 1 involves the identification of CBSIS through the safety Categorisation and Classification scheme. This is then refined by the application of IEC 62645 (Ref. 17) with cognisance of IEC 61226 to produce a Security Degree.
- Step 2 is the application of the appropriate elements of IEC 62645, 6.2 Requirements, 6.3 Planning, 6.4 Design and 6.9 Change Management. The other elements of IEC 62645 are appropriate to construction, operation and decommissioning of the systems.

- Step 3 determines whether the system is a contributing system to a VA which could result in an Unacceptable Radiological Consequence (URC) under DBT conditions.
- Step 4 is where a Cyber Risk Assessment will be carried out against the system in order to identify any design modifications to improve the security of the system.
- Step 5 is to conduct the change management process to deliver those design modifications.
- Step 6 will review all remaining systems against the DBT, to ensure supporting infrastructure is not at risk.
- Step 7 will review the physical protection of the CBSIS, with consideration of their location in relation to VAs.

3.5 Inventory of Nuclear Material (NM) and Other Radioactive Material (ORM)

26. This document details the expected inventory of NM and ORM for UK HPR1000 during its project lifecycle and is required as a key input into the VAI process. This inventory is expected to be expanded and refined as the UK-specific design is developed through future steps of the GDA. It is based on the reference plant for UK HPR1000, FCG 3. (Ref. 8)

3.6 Identified Operational Technology (OT)

27. This document consists of a list of CBSIS and their location. It is qualified that this list is subject to change as GDA progresses. (Ref. 9)

3.7 Definitions, Abbreviations and Acronyms

28. This document lists the terminology, abbreviations and acronyms used with all GSR associated documentation. This document will evolve as more terminology is referenced and used during the GDA. (Ref. 10)

3.8 Plant Information Record

29. The RP has also submitted, for information only, an outline of the proposed plant design. This will be subject to detailed assessment during GDA Step 3. (Ref. 12)

4 ONR ASSESSMENT

30. My Step 2 assessment work involved continuous engagement with the RP’s security specialists. This included two UK-based Technical Exchange Workshops and a number of Level 4 progress meetings. I also visited the subject matter experts, appointed by the RP to develop the VAI methodology and the Cyber Risk Assessment process.

31. During my GDA Step 2 assessment, I identified some gaps in the documentation formally submitted to ONR. Consistent with ONR’s Guidance to Requesting Parties (Ref. 18), these normally lead to Regulatory Queries (RQs) being issued. At the time of writing my Step 2 assessment report, I raised two RQs to facilitate my assessment. These were addressed promptly by the RP and closed out to my satisfaction.

32. Details of my GDA Step 2 assessment of the UK HPR1000 security arrangements, including the conclusions I have reached, are presented in the following sections of the report. This includes the areas of strength I have identified, as well as the items that require follow-up during subsequent steps of the GDA process.

4.1 The Security Case

4.1.1 Assessment

33. This section summarises my assessment of the Security Case (Ref. 2). I have assessed it against the agreed assessment plan (Ref. 1) and the guidance to RPs (Ref. 18).

34. The Security Case is in three parts, an overarching document and two annexes. Annex A (Ref. 3) summarises the relevant security claim and Annex B (Ref. 4) details which claims are in scope of the GDA process and which will be the responsibility of any subsequent licensee.

4.1.2 Strengths

35. In my opinion the documents clearly demonstrate the following:

- An understanding of the claims, arguments and evidence process now inherent in SyAPs. This should enable the RP to progress through Steps 3 and 4 of the GDA process.
- An understanding of the VAI process. This is essential when identifying areas of the facility which require the greatest levels of protection.

36. The RP has described in the Security Case and supporting annexes the proposed security arrangements for the reactor design. This included information on areas that ONR does not regulate directly. However, in my opinion, this holistic approach to security is likely to produce an enhanced security regime throughout the lifetime of the proposed reactor.

4.1.3 Items that Require Follow-up

37. During my GDA Step 2 assessment of the RP’s Security Case I identified the following additional potential shortfalls, to be followed up during Step 3 of the GDA:

- In my opinion the relationship between different levels of claims is not clear throughout the documents which have been submitted for assessment. As part of the Step 3 process, I will review the RP’s arguments relating to their methodology for the determination of different levels of individual claims.
- In my opinion the Security Case contains a significant amount of information not required during the GDA process. In my opinion, this could be beneficial to the RP and any subsequent licensee. However, in Step 3 of GDA, the RP will have to clarify which elements are both in and out of scope of Step 3 of the GDA assessment.
- Whilst ALARP is a well-established principle in the regulation of nuclear safety, it is not directly applied to the regulation of nuclear security. However, in some cases when the RP is determining whether risks to safety are ALARP, security factors may require consideration, so there is a need for some coordination. It should be noted that ALARP is a cross-cutting topic which is led by the Project Technical Inspector and is captured in the Summary of the Step 2 Assessment of the UK HPR1000 Reactor (Ref. 20).
- The application of deterrence to security arrangements is a fundamental security principle and, in my opinion, demonstrates a good understanding of security by the RP. However, due to the difficulties in measuring the effectiveness of deterrence, the RP will need to argue clearly how it will be used in Step 3 of the GDA process.

4.1.4 Conclusions

38. Based on the outcome of my Step 2 assessment of the Security Case, I have concluded that the claims are reasonable and of the type I would expect to see at this stage of the GDA process.

4.2 Security Risk Management Approach

4.2.1 Assessment

39. This document assesses the RP's approach to Security Risk Management (Ref. 5). It is supported by an annex (Ref. 6) describing specific details of the Risk Management Approach.

40. The RP has used the Risk Management Approach in formulating the VAI methodology.

41. I have assessed the Risk Management Approach against the agreed assessment plan (Ref. 1) and the Guidance to Requesting Parties document (Ref. 18).

4.2.2 Strengths

42. In my opinion the document clearly describes that the RP is protecting against the threats described in the NIMCA (Ref. 19).

4.2.3 Items that Require Follow-up

43. During my GDA Step 2 assessment of the Security Risk Management Approach, I identified the following areas that I will follow-up during Step 3 of GDA:

- The RP clearly breaks down the Detect aspect of the Deter, Detect and Delay security principle which, in my opinion, demonstrates a clear understanding of the concept. As the arguments develop during Step 3 of the GDA, I expect them to detail how the principle of Deter, Detect and Delay will be applied to the proposed security arrangements.
- Similarly, I am expecting the RP to present arguments regarding how it will be applying 'defence in depth' to the security arrangements.

4.2.4 Conclusions

44. Based on the outcome of my Step 2 assessment of the Security Risk Management Approach, I have concluded that the RP has demonstrated the necessary understanding of SyAPs and that this will adequately underpin the development of the VAI and Cyber Risk methodologies.

4.3 Vital Area Identification (VAI) methodology

4.3.1 Assessment

45. With the assistance of an appropriate subject matter expert in Security Informed Nuclear Safety (SINS), I have assessed the VAI methodology as proposed by the RP (Ref. 7) and the associated supporting documents. In my opinion, the VAI methodology has the potential to deliver a credible VAI submission, subject to its correct application to the UK specific design.

4.3.2 Strengths

46. In the VAI methodology document, the RP states that no credit will be taken for any security measures provided in undertaking the VAI work. In my opinion, this demonstrates that the RP has understood the VAI process and should be in a position to identify the areas of the plant requiring additional protective measures once this methodology is applied to the UK specific plant design.

4.3.3 Items that Require Follow-up

47. During my GDA Step 2 assessment of VAI methodology I identified the following areas that I will follow-up during Step 3 of GDA:

- The process described in the VAI methodology places a reliance on Suitably Qualified and Experienced Persons (SQEP). The RP will need to provide criteria for a Threat SQEP in a VAI context and demonstrate that those undertaking this role are adequately SQEP for the task.
- The VAI methodology states that the SQEP staff will utilise relevant recognised source information. The RP will need to demonstrate that the information used is relevant in the VAI context.

4.3.4 Conclusions

48. Based on my Step 2 assessment of the VAI methodology, I consider that the proposed methodology, at this stage of the GDA process, meets our expectations.

4.4 Cyber Security & Information Assurance Assessment

4.4.1 Assessment

49. With the assistance of an appropriate subject matter expert in CS&IA, I reviewed the documents submitted by GNS, particularly focusing on the documents identified in Section 3. The objective has been to confirm that the security case can go on to meet the objectives of SyDP 7.3, in that: "Dutyholders should ensure their operational and information technology is secure and resilient to cyber threats by integrating security into design, implementation, operation and maintenance activities" (Ref. 14). The exclusion of CBSy and IT is deemed appropriate for this stage. In Step 4 of the Cyber Risk Assessment process GNS has identified that a risk assessment is needed, but not identified a methodology (NIST SP 800-30, IRAM 2, IS1&2, Octave Allegro, etc.). Whilst not essential at GDA Step 2, as they progress through GDA, the use of a risk assessment methodology in this process will become more pressing as design modifications arise.

4.4.2 Strengths

50. GNS have opted to follow IEC 62645:2014 (Ref. 17) as the framework to evidence security by design through GDA and intend to use this framework in the operational phase of the new reactor. In my opinion, this new standard benefits from a wealth of learning gained in recent years regarding the application of cyber security in an industrial control system (ICS) environment.

4.4.3 Items that Require Follow-up

51. During my GDA Step 2 assessment of CS&IA I identified the following area that I will follow-up during GDA Step 3:

- The adequacy of the Cyber Risk Assessment methodology being used in Step 4 of the GNS Cyber Security Risk Assessment process.

4.4.4 Conclusions

52. Based on the outcome of my GDA Step 2 assessment of CS&IA, I have concluded that there is an appropriate process to take forward in GDA which is likely to produce sufficient evidence that the CBSIS on a UK HPR1000 site will be cyber secure by design.

4.5 Out of Scope Items

53. The following items have been left outside the scope of my GDA Step 2 assessment of the UK HPR1000 Security:

- Personnel Security. The reason for leaving this matter out of the scope of my GDA Step 2 assessment is that it will be the responsibility of any subsequent licensee.
- Perimeter (or site) security arrangements. The reason for leaving this matter out of the scope of my GDA Step 2 assessment is that it will be the responsibility of any subsequent licensee.

54. The above omissions do not invalidate the conclusions from my GDA Step 2 assessment. During my GDA Step 3 assessment, I will confirm the out-of-scope items as appropriate. I will capture this within my GDA Step 3 Assessment Plan.

4.6 Comparison with Standards, Guidance and Relevant Good Practice

55. In Section 2.2, above, I have listed the standards and criteria which I used during my GDA Step 2 assessment of the UK UKHPR1000 security, in order to judge the adequacy of the Preliminary Safety Report (Chapter 27) and supporting documents. In this regard, my overall conclusions can be summarised as follows:

- SyAPs. The RP has referenced SyAPs sufficiently in their submissions. This will need to be developed in the next step.
- TAGs. The RP has made reference to the VAI TAG and the TAG relating to the security assessment of generic new nuclear reactor designs. During subsequent steps, the RP may consider other relevant security TAGs which explain regulatory expectations.

4.7 Interactions with Other Regulators

56. Throughout my assessment I sought input from inspectors in a number of specialist areas, including CS&IA, C&I, VAI and ALARP. This approach will be continued in subsequent steps.

5 CONCLUSIONS AND RECOMMENDATIONS

5.1 Conclusions

57. During Step 2 of GDA, the RP submitted a PSR (Chapter 27) and supporting documents, which outline the proposed security arrangements for the UK HPR1000. These documents have been formally assessed by ONR. The PSR, together with its supporting submissions, adequately presents the claims which underpin the security arrangements of the UK HPR1000.

58. During Step 2 of GDA I have targeted my assessment at the content of the PSR and supporting submissions against the expectations of ONR's SyAPs, TAGs and other guidance, which ONR regards as RGP. From the UK HPR1000 assessment completed so far, I conclude the following:

- The RP has identified clearly a process by which the VAs and Cyber Risks can be identified. In my opinion, if correctly applied, this should allow the RP to identify accurately - and so mitigate - the most significant security risks to the reactor design.
- During Step 3 of the GDA process I will be assessing the RP's arguments relating to how they will apply the VAI and Cyber Risk Assessment process. In addition, throughout the documentation assessed above, the RP has made claims regarding the security of the facility which, in many cases, are not within the scope of the GDA. Whilst this breadth of approach could, in my opinion, lead to a significant increase in the security of the site once licensed, the RP, in Step 3, will need to be clear about which claims are in and out of scope of the GDA process.
- In my opinion, whilst the level of information provided by the RP is adequate for assessment in Step 2, the RP's understanding of the design will need to be developed in Steps 3 and 4 of the GDA process.

59. Overall, during my GDA Step 2 assessment, I have not identified any fundamental security shortfalls which might prevent the issue of a DAC for the UK HPR1000 design.

5.2 Recommendations

60. My recommendations are as follows.

- Recommendation 1: ONR should consider the findings of my assessment in deciding whether to proceed to Step 3 of GDA for the UK HPR1000.
- Recommendation 2: All the items identified in Step 2 as important to be followed up, should be included in ONR's GDA Step 3 Security Assessment Plan for the UK HPR1000.

6 REFERENCES

1. *Generic Design Assessment of GNS's UK HPR1000 - Step 2 Assessment Plan for Security* ONR-GDA-UKHPR1000-AP-17-006, Revision 0, ONR, November 2017. TRIM Ref 2017/351646.

2. *Security Case Report* UK HPR1000 - HPR-GDA-REPO-0064, GNS, TRIM Ref 2018/228806.

3. *Annex A to HPR-GDA-REPO-0064 Security Case Step 2 GSR Route Map* UK HPR1000 - GDA-REC-GNS-001903, GNS, TRIM Ref 2018/228810.

4. *Annex B to HPR-GDA-REPO-0064 - Security Case Claims and Arguments Table* UK HPR1000 - GDA-REC-GNS-001904, GNS, TRIM Ref 2018/228825.

5. *Security Risk Management Approach,* UK HPR1000 - HPR-GDA-REPO-0060, V0, GNS, TRIM Ref 2018/228823.

6. *Annex A to Security Risk Management Approach,* UK HPR1000 - HPR-GDA-REPO-0060, V0, GNS, TRIM Ref 2018/238668.

7. *Vital Area Identification Methodology,* UK HPR1000 - HPR-GDA-REPO-0062, GNS, TRIM Ref 2018/228815.

8. *NM/ORM Inventory,* UK HPR1000, GDA-REC-GNS-001865, GNS, TRIM Ref 2018/228814.

9. *Step 2 Identified Operational Technology List,* UK HPR1000 - GDA-REC-GNS-001866, GNS, TRIM Ref 2018/228818.

10. *GDA Project GSR Definitions,* UK HPR1000 - HPR-GDA-REPO-0065 UKHPR1000, V0, GNS, TRIM Ref 2018/228824.

11. *Generic Security Report V0 (Structure and Synopsis),* UK HPR1000 – HPR-GDA-REPO-0046, V0, GNS, TRIM Ref 2018/112513.

12. *Plant Information Record,* UK HPR1000 - GDA-REC-GNS-001872-GNS, V0, GNS, TRIM Ref 2018/228822.

13. *Revision 4 - Purpose and Scope of Permissioning,* ONR HOW2 Guide NS-PER-GD-014 July 2014. http://www.onr.org.uk/operational/assessment/index.htm

14. *Security Assessment Principles for the Civil Nuclear Industry*. 2017 Edition Revision 0. ONR, March 2017. http://www.onr.org.uk/syaps/index.htm

15. *Technical Assessment Guides*:
CNS-TAST-GD-6.1 (Rev 0) March 2020 Categorisation for Theft.
CNS-TAST-GD-6.2 (Rev 0) March 2020 Target Identification for Sabotage.
CNS-TAST-GD-6.3 (Rev 0) March 2020 Physical Protection System Design (OFFICIAL SENSITIVE).
CNS-TAST-GD-7.3 Protection of Nuclear Technology and Operations.
CNS-TAST-GD-11.1 (Rev 0) June 2020 Guidance on the Security Assessment of Generic New Nuclear Reactor Designs.
http://www.onr.org.uk/operational/tech_asst_guides/index.htm

16. *IAEA Guidance:*
IAEA Nuclear Security Series No.13 – Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5).
IAEA Nuclear Security Series No.16 – Identification of Vital Areas at Nuclear Facilities.
IAEA Nuclear Security Series 17 - Computer Security at Nuclear Facilities.
www.iaea.org.

17. *IEC Guidance:*
IEC 62645 Nuclear power plants - Instrumentation and control systems - Requirements for security programmes for computer-based systems.
IEC 61226 Nuclear power plants. Instrumentation and control systems important to safety. Classification of instrumentation and control functions.
http://www.iec.ch/

18. *New nuclear reactors: Generic Design Assessment - Guidance to Requesting Parties.* ONR-GDA-GD-001 Revision 3, ONR, September 2016. http://www.onr.org.uk/new-reactors/ngn03.pdf

19. *Nuclear Industries Malicious Capabilities (Planning) Assumptions* (2017/2018 review), ONR.

20. *ONR, Summary of the Step 2 Assessment of the UK HPR1000 Reactor*, ONR-GDAUKHPR1000- AR-18-020, ONR, TRIM 2018/238474.

21. *UK HPR1000 Preliminary Safety Report* (PSR) Chapter 27, CGN/GNS, November 2017.