Office for Nuclear Regulation

An agency of HSE

Generic Design Assessment – New Civil Reactor Build

Step 4 Security Assessment of the Westinghouse AP1000® Reactor

Assessment Report: ONR-GDA-AR-11-015
Revision 0
10 November 2011

COPYRIGHT

First published November 2011

PREFACE

The Office for Nuclear Regulation (ONR) was created on 1st April 2011 as an Agency of the Health and Safety Executive (HSE). It was formed from HSE's Nuclear Directorate (ND) and has the same role. Any references in this document to the Nuclear Directorate (ND), the Nuclear Installations Inspectorate (NII) or the Office for Civil Nuclear Security (OCNS) should be taken as references to ONR.

The assessments supporting this report, undertaken as part of our Generic Design Assessment (GDA) process, and the submissions made by Westinghouse relating to the AP1000® reactor design, were established prior to the events at Fukushima, Japan. Therefore, this report makes no reference to Fukushima in any of its findings or conclusions. However, ONR has raised a GDA Issue which requires Westinghouse to demonstrate how they will be taking account of the lessons learnt from the events at Fukushima, including those lessons and recommendations that are identified in the ONR Chief Inspector's interim and final reports. The details of this GDA Issue can be found on the Joint Regulators' new build website www.hse.gov.uk/newreactors and in ONR's Step 4 Cross-cutting Topics Assessment of the AP1000® reactor.

EXECUTIVE SUMMARY

This report presents the findings of the Security Assessment of the Westinghouse AP1000 reactor undertaken as part of Step 4 of the Health and Safety Executive's Generic Design Assessment. The assessment is based on the supporting documentation submitted by Westinghouse during Step 4 and the previous steps.

The assessment followed a step-wise-approach in a claims-argument-evidence hierarchy. In Step 2 the claims made by Westinghouse were examined and in Step 3 the arguments that underpin those claims were examined.

The scope of the Step 4 Assessment was to review the Security aspects of the AP1000 reactor in greater detail, by examining the evidence, supporting arguments and claims made in the security documentation, building on the assessments already carried out for Steps 2 and 3, and to make a judgement on the adequacy of the security proposals contained within the security documentation.

The Step 4 assessment focussed on:

- Vital Area Identification and related security measures (physical and electronic);
- Computer Based Systems Important to Nuclear Safety and the physical security of the associated equipment; and
- Conceptual Security Arrangements proposed by Westinghouse.

A number of plant items have been agreed with Westinghouse as being outside the scope of the Generic Design Assessment process and hence have not been included in the assessment.

Overall, based on the review undertaken we are satisfied that the claims, arguments and evidence laid down within the documentation submitted as part of the Generic Design Assessment process presents an adequate security case for the generic AP1000 reactor design. The AP1000 reactor is therefore considered suitable from a security perspective for construction in the UK, subject to satisfactory progression and resolution of Generic Design Assessment Findings, listed in Annex 1, to be addressed during the forward programme for this reactor. There are also a number of findings that will require project developers or Site Licensees proposing to use this technology in the UK to progress as these are site specific issues.

The Office for Nuclear Regulation, Civil Nuclear Security, would require to receive updated information for review should the AP1000 have material changes made to the design.

The security measures for the generic elements of the AP1000 design form a part of the overall security infrastructure that will be required for the application of this technology at a specific UK location. The project developers or Site Licensees will be required to incorporate these generic elements, identified in the Westinghouse Conceptual Security Arrangements submission into the overall Site Security Arrangements.

LIST OF ABBREVIATIONS

CBSIS	Computer Based Systems Important to Nuclear Safety
C, I & A	Confidentiality, Integrity and Availability
C&I	Control and Instrumentation
CNS	Civil Nuclear Security
CSA	Conceptual Security Arrangements
DECC	Department of Energy and Climate Change
ERL	Emergency Reference Level
GDA	Generic Design Assessment
HSA	High Security Area
HSE	Health and Safety Executive
IAEA	International Atomic Energy Agency
I & A	Integrity and Availability
ILW	Intermediate Level Waste
ND	(HSE) Nuclear Directorate
NIMCA	Nuclear Industries Malicious Capabilities Planning Assumptions
NISR	Nuclear Industries Security Regulations
NM	Nuclear Material
OCNS	Office for Civil Nuclear Security
ONR	Office for Nuclear Regulation
ONR (CNS)	formally Office for Civil Nuclear Security
ORM	Other Radioactive Material
PCSR	Pre-construction Safety Report
PCER	Pre-construction Environmental Report
PMI	Protectively Marked Information
SAP	Safety Assessment Principle
SSC	System, Structure and Component
TQ	Technical Query
TRD	Technical Requirements Document
TSC	Technical Support Contractor
VA	Vital Area
VAI	Vital Area Identification
US NRC	Nuclear Regulatory Commission (United States of America)

TABLE OF CONTENTS

1 INTRODUCTION 1
2 NUCLEAR DIRECTORATE'S ASSESSMENT STRATEGY FOR SECURITY 3
2.1 Assessment Plan 3
2.2 Standards and Criteria 5
2.3 Assessment Scope 5
2.3.1 Findings from GDA Step 3 5
2.3.2 Additional Areas for Step 4 Security Assessment 5
2.3.3 Use of Technical Support Contractors 6
2.3.4 Cross-cutting Topics 6
2.3.5 Integration with Other Assessment Topics 6
2.3.6 Out of Scope Items 7
3 WESTINGHOUSE - SECURITY SUBMISSIONS 8
3.1 Westinghouse - Vital Area Identification 8
3.2 Westinghouse's Computer Based System Important to Nuclear Safety 8
3.3 Westinghouse - Conceptual Security Arrangements 9
4 GDA STEP 4 NUCLEAR DIRECTORATE ASSESSMENT FOR SECURITY 10
4.1 Vital Area Identification 10
4.1.1 Assessment 10
4.1.2 Findings 10
4.2 Computer Based Systems Important to Nuclear Safety 10
4.2.1 Assessment 11
4.2.2 Findings 11
4.3 Conceptual Security Arrangements 11
4.3.1 Assessment 11
4.3.2 Findings 11
4.4 Overseas Regulatory Interface 14
4.5 Multilateral Collaboration 15
4.6 Interface with Other Regulators 15
4.7 Other Relevant Legislation and Guidance 15
5 CONCLUSIONS 17
5.1 Key Findings from the Step 4 Assessment 17
5.1.1 Assessment Findings 17
5.1.2 GDA Issues 17
6 REFERENCES 18

Tables

Table 1: GDA Supporting Documentation for Security Sampled during Step 4
Table 2: Relevant Security Policy Documents Considered During Step 4

Annexes

Annex 1: Assessment Findings to be Resolved During the Forward Programme as Normal Regulatory Business – Security – AP1000

Annex 2: GDA Issues – Security – AP1000

1 INTRODUCTION

1 This report presents the Security Assessment findings for the Westinghouse AP1000 reactor. It has followed the process that was given in the Office for Civil Nuclear Security (OCNS) (now Office for Nuclear Regulation, Civil Nuclear Security (ONR (CNS))) guidance document, (Ref. 1) subsequently developed in a letter sent to Westinghouse (Westinghouse) (Ref. 4). This report concentrates mainly on the Vital Area Identification (VAI) and Conceptual Security Arrangements (CSA) for the Westinghouse AP1000 reactor, and the supporting documentation provided by Westinghouse (Westinghouse) under the Office for Nuclear Regulation (ONR) Generic Design Assessment (GDA) process.

2 The assessment took into account the Safeguards Assessment Report (Ref. 14) and its subsequent updates (Refs 15, 16 and 17) that contain details of the VAI process for the AP1000 and supporting documents (Refs 18, 19, 20, 21 and 27), and the CSA (Ref. 22) and its subsequent updates (Refs 23 and 29). The approach taken was to review the submissions, and undertake a technical security assessment of the relevant documentation and proposals contained within. The extant version of the Nuclear Industries Malicious Capabilities Planning Assumptions[1] (NIMCA) document (Ref. 5) and the security objectives, requirements and model standards contained within the Nuclear Industries Security Regulations (NISR) 2003, Technical Requirements Document (TRD) Part Seven (Ref. 6) were taken into account during the assessment. Ultimately, the goal of the assessment was to reach an independent and informed judgment on the adequacy of the physical and technical security measures in the generic reactor design.

3 During the assessment, OCNS corresponded with Westinghouse by letter on several occasions requesting additional information. Periodic meetings were also held between OCNS and Westinghouse to promote understanding, discuss progress and agree the next steps. The Technical Queries (TQ) process was not used during the process due to the security sensitivity of some aspects of the subject matter, the need for the queries and replies to be managed on a strict 'need to know' and to be protectively marked in accordance with classification policy (Ref. 7).

4 A number of plant items were agreed with Westinghouse as being outside the scope of the GDA process and these have not been included in this assessment. These include, but are not limited to, the physical security measures for the High Security Area (HSA) boundary within which the nuclear island will be contained, and the long-term storage facilities for spent nuclear fuel and intermediate level waste[2].

5 The International Atomic Energy Agency (IAEA), 'through its Nuclear Security Programme supports States to establish, maintain and sustain an effective security regime'. Recommendations in INFCIRC/225/Rev.4 (Ref. 10) and INFCIRC/225/Revison 5 (Ref. 11) particularly Chapter 7, in the former and Chapters 3 and 5 of the latter were taken into account during the assessment.

6 The assessment report is Not Protectively Marked and measures in Section 79 of the Anti-terrorism, Crime and Security Act 2001 (Ref. 9) were considered regarding the prohibition on disclosure of information relating to nuclear security[3]. ONR (CNS) has provided as much information as practicable in this report without releasing protectively

[1] Fundamental Principle G: Threat – INFCIRC/225/Revision 5 (Ref. 11).

[2] See also the Step 4 Assessment Report for Radioactive Waste and Decommissioning (Ref. 30).

[3] Supporting Fundamental Principle L: Confidentiality – INFCIRC/225/Revision 5 (Ref. 11).

marked information (PMI), originated by the United Kingdom or the United States of America. Consequently, general assessment findings are discussed in the following paragraphs as opposed to detail on specific security requirements that are built into the design and any that will be required to be in place if an AP1000 reactor is built in the United Kingdom.

2 NUCLEAR DIRECTORATE'S ASSESSMENT STRATEGY FOR SECURITY

7 The assessment strategy for Step 4 for the Security topic area was set out in an assessment plan (Ref. 2). This identified the intended scope of the assessment, standards and criteria to be applied which are discussed in the following paragraphs.

2.1 Assessment Plan

8 The assessment plan concentrated on VAI, the identification of the physical locations of the Computer Based Systems Important to Nuclear Safety (CBSIS), the identification of the existing security arrangements in the generic design and the validation of Westinghouse's Conceptual Security Arrangements (CSA).

9 VAI is linked to the graded approach[4] to radiological consequences for sabotage (Ref. 11) where it is considered that terrorists, malcontents or individuals (including insiders) could attempt to carry out an act of sabotage against a site involving Nuclear Material (NM), Other Radioactive Materials (ORM), or any other identified Vital Areas (VAs), in such a manner as to create an unacceptable radiological hazard to employees and/or the public (see paragraph 18). At some sites, including nuclear power stations, an act of sabotage involving NM/ORM held on the site, or against specific Systems, Structures or Components (SSC) comprising part of the site's infrastructure could create (without appropriate security measures) a radiological hazard to the public and/or environment. At such sites, the potential for sabotage and the associated potential radiological consequences is to be evaluated by the operators' safety specialists, in close consultation with their security counterparts and ONR Safety and Security specialists. The purpose of the evaluation is to identify the potential VAs to be protected by appropriate security measures, using the graded approach, depending on the potential (low, medium or high) consequences of a successful sabotage attack.

10 The UK definition of a VA is 'An area containing nuclear material and/or other radioactive material (including radioactive sources) or equipment, systems, structures or devices the sabotage or failure of which, alone or in combination, through malevolent acts as defined in the extant NIMCA document (Ref. 5), could directly or indirectly result in unacceptable radiological consequences, thereby potentially endangering public health and safety by exposure to radiation' (Ref. 6).

11 CBSIS are to be protected against cyber attack, manipulation, falsification or sabotage (Ref. 6) consistent with the threat assessment and the malicious capabilities detailed in the NIMCA document. This implements the recommendation at paragraph 5.19 of INFCIRC/225/Revision 5. It is imperative that the operators, in this case Westinghouse, identify CBSIS, so security requirements for these systems can be identified. A CBSIS is a system that falls into one or both of the following categories:

- **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.
- **Safety-related systems:** Any other computer systems that could through their actions or lack thereof, have an adverse affect on the safety of a nuclear system (e.g. a

[4] Fundamental Principle H: Graded Approach – INFCIRC/225/Revision 5 (Ref. 11).

control system that maintains working parameters within pre-defined limits by responding continuously to normal plant operations).

12 The Control and Instrumentation (C&I) assessment has been influential in identifying the systems that require enhanced protection. The CSA submission should have identified the physical locations of these systems and detailed the physical security measures for their protection, to support their availability.

13 The protection of other aspects of these systems is being addressed by the C&I assessment within GDA and Site Licensees will need to ensure that Information Security requirements set in policy by ONR are met throughout the design, construction and operation phases.

14 The CSA are proposed by Westinghouse and validated by the ONR (CNS), similarly to the Pre-construction Safety Report (PCSR) and the ONR Safety Regulator and Pre-construction Environmental Report (PCER) and the Environmental Regulator. The CSA document:

- Identifies potential VAs, (to be considered in line with the UK definition).
- Provides details of CBSIS present in the design, including those that may be dependent on specific site features.
- Contains sufficient technical information on these topics so a clear understanding can be gained on all relevant issues. Drawings and plans should be used to detail where these elements are physically located in the generic design.
- Includes sufficient information on access control arrangements, including emergency exits, particularly in areas containing VAs and CBSIS. It must be clear how movement into and out of the security zones/areas is controlled and drawings are to identify the location of all external and internal security doors, including those used for emergency purposes. Emergency egress routes into and out of secure areas are also required to be detailed in order that proposed security arrangements are not compromised for safety.

15 The CSA document and associated drawings are to provide information of those aspects of 'defence in depth'[5] that are related to the generic design. It is to detail any security features that will be used either locally or remotely to control access to VAs and to CBSIS. The construction details of the walls, floors or ceilings of those areas that house and adjoin areas containing VAs and CBSIS need to be detailed, together with any security features built into the design to delay and detect unauthorised intrusion. Security access control arrangements for the different plant states (commissioning, normal operations, maintenance and outage) should also be detailed and work in this area is ongoing between Westinghouse and ONR (CNS).

16 Aircraft Impact is not considered as a part of the Security Assessment. However, this subject is addressed under the Civil Engineering and External Hazards topic areas and detailed in Step 4 Assessment Report ONR-GDA-AR-11-002 (Ref. 31). The transfer and control of PMI between Westinghouse and HSE ND on this subject area has complied with the protective security measures as regulated by ONR (CNS).

17 The conventional safety review has not been carried out as part of the GDA process. This will be undertaken during the site licensing phase. Decisions, particularly in relation

[5] Fundamental Principle I: Defence in depth – INFCIRC/225/Revision 5 (Ref. 11).

to fire escape routes that may affect security, and the arrangements in the CSA, will need to be discussed with ONR (CNS) (Assessment Finding **AF-AP1000-SEC-13**).

> **AF-AP1000-SEC-13:** *The Site Licensee will need to determine that the emergency routes confirm to UK requirements and ensure that security measures are not compromised.*
>
> This assessment finding should be addressed as part of the following procurement and construction generic milestone for assessment findings:
>
> - Nuclear island safety related concrete.

2.2 Standards and Criteria

18 The standards and criteria for the identification of VAs are determined by ONR nuclear safety specialists. In the United Kingdom, a dose rate of more than 30 milliSieverts (mSv), unaverted over a 24 hour period at a site's perimeter is considered as unacceptable. This is the upper level at which the Health Protection Agency Emergency Reference Levels[6] (ERLs) Countermeasure Organ Dose Level in mSv for the whole body for sheltering and the lower ERL for evacuation.

19 The requirements for the content of the CSA document were provided in the CSA guidance document sent to Westinghouse with letter WEC70144R dated 3 February 2010 (Ref. 4).

20 The identification of the CBSIS systems was carried out by Westinghouse and validated by the ONR Safety Assessor for Control and Instrumentation (C & I). The standards and criteria are detailed in the Step 4 C&I Assessment Report (Ref. 32).

2.3 Assessment Scope

21 The assessment in Step 4 covered relevant aspects of the VAI and CSA submissions. ONR (CNS) had to confirm that all the VAs validated by others in ONR were sufficiently detailed in the CSA and adequate security measures will be built into the design for protection against malicious capabilities and threats as required by Safety Assessment Principles (SAPs) and as detailed in the NIMCA.

2.3.1 Findings from GDA Step 3

22 Security assessment work in Step 3 (Ref. 3) primarily concentrated on reviewing the submission for the VAI and identifying those areas where clarification or expansion would be required in the Westinghouse submission.

2.3.2 Additional Areas for Step 4 Security Assessment

23 The Step 4 Security Assessment expanded on the VAI work. Work on CBSIS was also undertaken in consultation with ONR Safety Assessors and finally the CSA document was reviewed in detail.

---

[6] 'ERLs have been formulated using a two tier system. For each urgent countermeasure there are a lower and an upper level of dose saving. For doses below the lower level the countermeasure is unlikely to be worthwhile, above the upper level it would be worthwhile in most circumstances and at doses between the lower and upper level the implementation of the countermeasure would be desirable'. (Department of Energy and Climate Change (DECC) Fact Sheet 10).

2.3.3 Use of Technical Support Contractors

24 No external Technical Support Contractors (TSC) were used during the VAI or to provide any input to the CSA document. However, TSCs were used in the Civil Engineering, External Hazards, and Control and Instrumentation assessments that assisted in informing parts of the security assessment work. TSCs may also have been used in other assessments (Section 2.3.5) that may have had an influence on the outcome of the Security Assessment.

2.3.4 Cross-cutting Topics

25 The following Cross-cutting Topics have been considered within this report:

Fault Studies

The failure of structures, systems and components in isolation or in combination, due to natural or malicious causes, resulting in unacceptable radiological consequences was an area of interest in the Security Assessment.

However, the confirmation, or otherwise, of the consequences of the failure to SSCs was carried out by safety assessors and the results were considered when validating the VAI report (Ref. 14).

2.3.5 Integration with Other Assessment Topics

26 ONR (CNS) has interacted with the following assessment areas during the Security Assessment by discussing areas of common interest and assisting these assessments as required, with the management of PMI.

27 **External Hazards**

- Aircraft impact
- Explosion and the effect of blast

28 **Internal Hazards**

- Fire
- Flooding
- Internal missiles generated through plant failures

29 **Control and Instrumentation**

- Computer Based Systems Important to Nuclear Safety (CBSIS)

30 **Probabilistic Safety Analysis**

- Multiple failures and the resulting consequences

31 **Fault Studies**

- Individual and multiple failures and the resulting consequences

32 **Civil Engineering**

- Physical properties of building structures

2.3.6 Out of Scope Items

33 The following items were agreed with Westinghouse as being outside the scope of GDA:

- The long-term storage facilities for spent nuclear fuel.
- The long-term storage facilities for Intermediate Level Waste (ILW).
- Site specific systems contributing to nuclear safety and security and their associated equipment.

3 WESTINGHOUSE - SECURITY SUBMISSIONS

3.1 Westinghouse - Vital Area Identification

34 The VAI documents (Refs 14, 15, 16 and 17) and the AP1000 Vital Equipment List (Ref. 19) all protectively marked SAFEGUARD INFORMATION, were treated as equivalent to UK CONFIDENTIAL, and were supplied directly to ONR (CNS).

35 The NIMCA document is protectively marked with a UK EYES ONLY caveat and could not be shared with Westinghouse. However, the methodologies used to identify potential VAs were shared.

36 ONR Security and Safety Specialists worked together to ensure that the threats postulated in NIMCA were being adequately addressed through the VAI assessment. The agreement from ONR Safety specialists that the VAI document adequately identified the Vital Areas (systems, structures and components) in the generic design is at Ref. 28.

37 ONR Safety specialists also supported the Security Assessment process to identify CBSIS.

38 A number of safety specialists assisted in the Security Assessment. These were mainly specialists working on those parts of the assessment concerned with Internal Hazards, External Hazards, Civil Engineering, Mechanical Engineering, Structural Integrity, Electrical Engineering and Systems, Control and Instrumentation, Fault Studies and Severe Accidents.

3.2 Westinghouse's Computer Based System Important to Nuclear Safety

39 Documentation submitted to address some areas of CBSIS in GDA were Refs 24 and 25.

40 The protection of CBSIS is to address how the system(s) are protected against cyber attack, manipulation, falsification or sabotage (Ref. 6) so as to maintain their Confidentiality, Integrity and Availability (C, I & A) (Ref. 8).

- **Confidentiality.** The restriction of information and assets to authorised individuals.
- **Integrity.** The maintenance of information systems and physical assets in their complete and proper form.
- **Availability.** The continuous or timely access to information, systems or physical assets by authorised individuals.

41 The Security Assessment in GDA determined the physical security measures to ensure Integrity and Availability. Some aspects of the Confidentiality Issues and the protection against cyber attack, manipulation and falsification have been addressed by Control and Instrumentation (C & I) specialists in GDA. Further work will also be required by the relevant specialists during the Site Licensing process (Assessment Finding **AF-AP1000-SEC-14**).

> **AF-AP1000-SEC-14:** *The Site Licensee will need to protect CBSIS against cyber attack, manipulation and falsification to the appropriate Information Security standards as determined by ONR (CNS).*
>
> This assessment finding should be addressed as part of the following procurement and construction generic milestone for assessment findings:
>
> - Mechanical, Electrical and C&I Safety Systems – before delivery to site.

42 The verification of CBSIS in GDA was undertaken by Control and Instrumentation assessors. They are reporting separately. However, their assistance has helped confirm the CBSIS components that require additional protection.

3.3 Westinghouse - Conceptual Security Arrangements

43 The submitted versions of the Conceptual Security Arrangements (CSA) document (Refs 22, 23 and 29) are protectively marked and contain sections on:

- Overview of the Plant Security System.
- Vital Area Identification.
- Computer Based Systems Important to Nuclear Safety (CBSIS).
- Security Barrier Identification.
- Access Control into and around the nuclear island and Vital Areas.
- Associated drawings and tables.

44 The initial guidance for the Security Assessment of the generic design can be found at Ref. 1.

45 Guidance on the content and layout of the Conceptual Security Arrangements document was sent to Westinghouse in letter WEC70144R dated 3 February 2010 (Ref. 4). Subsequent meetings have been undertaken to support Westinghouse's development of the CSA document for the AP1000.

46 Comments on Revision A of the CSA (Ref. 22) are contained in WEC70275R dated 15 December 2010 (Ref. 12). Revision B of the CSA document (Ref. 23) has been reassessed with comments contained within Revision A of the Step 4 Security Technical Assessment report (Ref. 13). Revision 3 of the CSA (Ref. 29) has been assessed.

4 GDA STEP 4 NUCLEAR DIRECTORATE ASSESSMENT FOR SECURITY

4.1 Vital Area Identification

47 The VAI task was to determine those SSCs that could, if damaged cause unacceptable radiological consequences (see paragraph 18). Westinghouse carried out an analysis of their plant and produced a report detailing the methodology they used and the VAs identified.

48 ONR (CNS), with assistance from ONR Safety specialists assessed the report.

4.1.1 Assessment

49 The initial VAI report (Ref. 14) which was submitted identifying the VAs in the AP1000 design was assessed by both OCNS and ONR Safety Assessors. The Safety Assessors helped validate the methodology used and confirmed the accuracy and completeness of the identified VAs.

50 Subsequent updates (Refs 15, 16 and 17) were reviewed to ensure that changes remained consistent with the earlier versions and any significant amendments were thoroughly assessed by ONR Security and Safety specialists.

4.1.2 Findings

51 The VAI reports (Refs 14, 15, 16 and 17) categorised SSCs into target sets following the recommendations in INFCIRC/225/Revision 5. Those target sets were then analysed with the consequences of their failure determined, the adversary action that would need to be carried out detailed, and the anticipated results summarised.

52 During the assessment, Security and Safety Assessors working together, decided that the SSCs detailed in the reports (Refs 14, 15, 16 and 17) constituted those Vital Areas that could be determined in the scope of GDA (Ref. 28).

53 The assessment has confirmed that the site specific VAI should lead to the decision on whether potential VAs can be confirmed as VAs or not. It has also confirmed that it is easier to present evidence as to why a SSC is ‘vital’ than it is to present or demonstrate why a SSC is ‘not-vital’.

54 Westinghouse considered that some aspects of plant are not Vital Areas and this will need to be confirmed by a Site Licensee during their VAI process.

55 Westinghouse carried out its assessment without being in possession of the specific malicious capabilities detailed in the NIMCA document. Although it was thought that the determination of what is or is not ‘Vital’ could not be done without the specific malicious threats, the robust methodology used, looking beyond the conventional plant failure accidents, was effective in identifying the significant SSCs that could lead to unacceptable radiological consequences.

4.2 Computer Based Systems Important to Nuclear Safety

56 Computer Based Systems Important to Nuclear Safety (CBSIS) will require to be protected to ensure Integrity and Availability (I & A), so that they can perform their function when required. As part of the Security Assessment in GDA, the CBSIS will need to be identified (and work in this area is progressing) so that important nodal locations are

determined. The physical security measures at those locations are still to be fully assessed to ensure adequate physical protection.

57 As the specific equipment that constitutes the CBSIS is not yet fully determined, the Information Security measures to ensure Confidentiality, Integrity and Availability (C, I & A) (see paragraph 40) will be determined during Site Licensing and construction.

4.2.1 Assessment

58 The Security Assessment of CBSIS in GDA has concentrated on the identification of physical locations where CBSIS equipment must be protected to ensure that unauthorised access to the equipment does not compromise I & A.

4.2.2 Findings

59 The locations of CBSIS equipment that requires physical and access control arrangements to prevent unauthorised access to the equipment are shown in the drawings and this constitutes PMI.

60 The robustness of the areas containing this equipment, including access points, will also need to meet the required physical resistance to forcible attack.

4.3 Conceptual Security Arrangements

61 The completed CSA document for the AP1000 is to detail:

- the locations of the potential VAs requiring protection;
- identify the proposed physical security protection measures for those VAs;
- the access control measures for the nuclear island and the VAs; and
- the same information for CBSIS.

62 This CSA document will constitute the basis of the ‘defence in depth’ strategy that will be developed by the Site Licensee.

4.3.1 Assessment

63 The CSA document was assessed against the required contents and the specific details on VAI, CBSIS and the Access Control measures presented.

4.3.2 Findings

64 The detailed findings and actions on Revision B of the CSA document (Ref. 23) are in Revision A of the protectively marked technical report at Ref. 13.

65 Issue C of the CSA (Ref. 29) took account of the findings in Revision A of Ref. 13. Issue C has been assessed by ONR (CNS) and is deemed to provide a robust and acceptable submission that meets the regulatory requirements.

66 The general findings on the CSA that will need to be addressed during the forward programme as normal regulatory business are given below.

67 Vital Area Identification (VAI)

- The potential VAs identified are considered to be an adequate list in the AP1000 design subject to GDA assessment.
- The VAI submission has been validated by ONR Safety specialists for the GDA assessment who consider that it 'adequately identified Vital Areas for the Generic Design' (Ref. 28).
- Acknowledgement is made in the CSA that Site Licensees will need to revalidate the findings taking into account the NIMCA document (Ref. 5). Site Licensees will also need to carry out a VAI for items of plant not covered by the GDA (Assessment Finding **AF-AP1000-SEC-04**).

  AF-AP1000-SEC-04: *The Site Licensee will need to carry out their own Vital Area Identification process taking into account the extent of the relevant malicious capabilities in NIMCA that need to be considered to validate the Westinghouse VA list and confirm that no VAs are created for the site specific application of the AP1000 technology not identified in GDA.*

  This assessment finding should be addressed as part of the following procurement and construction generic milestone for assessment findings:

  - First structural concrete.

68 Computer Based Systems Important to Nuclear Safety (CBSIS)

- Protection of CBSIS against cyber attack, manipulation and falsification will require to be completed by the relevant specialists during the site licensing process (Assessment Finding **AF-AP1000-SEC-14**) (see paragraph 41).

69 Access Control

- Access control drawings correctly identify the boundary between GDA and the Licensee's Security Arrangements. Proposed access control arrangements shown that are within the 'Limits of the Licensee's Security Arrangements' are beyond the scope of this ONR (CNS) assessment.
- Specific equipment for access control and associated operating procedures will be determined through interaction with Site Licensees (Assessment Finding **AF-AP1000-SEC-10**).

  AF-AP1000-SEC-10: *The Site Licensee will need to determine the specific AACS equipment that will be needed to meet the requirements in TRD.*

  This assessment finding should be addressed as part of the following procurement and construction generic milestone for assessment findings:

  - Install RPV.

70 Physical Security Systems

- The doors, locking mechanisms and other physical security measures designed to resist forcible attack will need to meet the required protection levels and the Class requirements against surreptitious attack, as detailed in TRD Part Seven (Ref. 6) (Assessment Findings **AF-AP1000-SEC-02** and **AF-AP1000-SEC-09**).

  AF-AP1000-SEC-02: *The Site Licensee should make themselves aware of the security objectives and requirements in the extant Technical Requirements Document, Part Seven, or any replacement.*

This assessment finding should be addressed as part of the following procurement and construction generic milestone for assessment findings:

- First structural concrete.

AF-AP1000-SEC-09: *The Site Licensee will need confirm and provide evidence that the security doors to be installed meet the performance requirements in TRD.*

This assessment finding should be addressed as part of the following procurement and construction generic milestone for assessment findings:

- Install RPV.

71 Technical Security Systems

- Systems for Detection, Closed Circuit Television and Automatic Access Control for the protection of VAs and the nuclear island will need to meet the performance requirements detailed in the TRD Part Seven (Ref. 6) (Assessment Findings **AF-AP1000-SEC-05** and **AF-AP1000-SEC-10**).

  AF-AP1000-SEC-05: *The Site Licensee will need to demonstrate that the Technical Security Systems design(s) will meet the requirements of TRD.*

  This assessment finding should be addressed as part of the following procurement and construction generic milestone for assessment findings:

  - Install RPV.

  AF-AP1000-SEC-10: *See paragraph 69.*

- The location of the Security Force Control Room and the Auxiliary Security Force Control Room where the integrated security system is monitored and the automatic access control system is managed will be decided in the site specific phase (Assessment Finding **AF-AP1000-SEC-03**).

  AF-AP1000-SEC-03: *The Site Licensee will need to address site specific issues, such as the location of the Security Force Control Centre, while developing the Construction Security Plan and site layout.*

  This assessment finding should be addressed as part of the following procurement and construction generic milestone for assessment findings:

  - First structural concrete.

- The standby and long term backup supplies for the security infrastructure will be determined by Site Licensees (Assessment Finding **AF-AP1000-SEC-06**).

  AF-AP1000-SEC-06: *The Site Licensee will need to engineer long term power supply to support the security infrastructure and demonstrate its adequacy.*

  This assessment finding should be addressed as part of the following procurement and construction generic milestone for assessment findings:

  - Install RPV.

72 Site Specific Changes

- Changes to site specific building, such as changes to the Turbine Hall for housing 50 Hz turbines compared to the American 60 Hz turbines, must be demonstrated not to compromise the generic security arrangements (Assessment Finding **AF-AP1000-SEC-01**).

AF-AP1000-SEC-01: *The Site Licensee are to demonstrate that generic security features are unaffected by site specific arrangements.*

This assessment finding should be addressed as part of the following procurement and construction generic milestone for assessment findings:

- First structural concrete.

73 Site Specific Measures and Procedures

- The physical, technical and procedural arrangements for the site will be complemented by the responses force. As the physical elements will need to provide adequate delay to allow an appropriate response by the security force a vulnerability assessments will need to be undertaken (Assessment Finding **AF-AP1000-SEC-08**).

  AF-AP1000-SEC-08: *The Site Licensee will need to carry out a vulnerability assessment for their proposed site layout and security force staffing to confirm and demonstrate that the measures in the CSA continue to meet the security objectives in TRD Part Seven.*

  This assessment finding should be addressed as part of the following procurement and construction generic milestone for assessment findings:

  - Nuclear island safety related concrete.

- Search arrangements to prevent the introduction of unauthorised materials onto site and into secure areas are mandated in TRD Part Seven (Ref. 6) and will need to compliment the physical security measures (Assessment Finding **AF-AP1000-SEC-11**).

  AF-AP1000-SEC-11: *The Site Licensee will need to ensure that searching requirements in TRD Part Seven can be fulfilled.*

  This assessment finding should be addressed as part of the following procurement and construction generic milestone for assessment findings:

  - Install RPV.

- Access arrangements (under all operating conditions) to Containment will need to be developed to ensure that physical security measures are not compromised (Assessment Finding **AF-AP1000-SEC-12**).

  AF-AP1000-SEC-12: *The Site Licensee will need to develop procedures to meet the security objectives for access to the Containment Building under all plant conditions.*

  This assessment finding should be addressed as part of the following procurement and construction generic milestone for assessment findings:

  - Fuel on-site.

4.4 Overseas Regulatory Interface

74 OCNS have been working effectively with the US Nuclear Regulatory Commission (US NRC) in managing the transfer of classified information between ONR and Westinghouse, when necessary.

4.5 Multilateral Collaboration

75 ONR (CNS) collaborates in the work of the International Atomic Energy Agency (IAEA) in the area of Nuclear Security. Among the activities ONR (CNS) staff have contributed to is the updating of INFCIRC/225 Revision 4 to Revision 5. Staff have participated in the open-ended technical meetings during its development, provided comments during the consultation stage and attended the open-ended technical review meeting where the final revision was agreed. This work has promoted consistent nuclear security standards in the UK and has strengthened Nuclear Security internationally.

4.6 Interface with Other Regulators

76 ONR (CNS) has worked closely with ONR Safety specialists, on many aspects of the GDA assessments. This has included participation in joint assessment, project and management meetings, and dealing with the handling, storage, transmission, marking and management of PMI.

77 Throughout GDA there has been cooperation with the Environment Agency assessors and management, particularly on project management and PMI issues.

4.7 Other Relevant Legislation and Guidance

78 The Nuclear Industries Security Regulations 2003 (NISR 20003) Statutory Instrument 2003 No. 403.

- These regulations were made under the Anti-terrorism, Crime and Security Act 2001, to reform the civil nuclear security regulatory framework. The regulations provide a clear, unified approvals regime for nuclear security and for assessing compliance with approved security plans.
- The enforcement provisions of the regulations apply which broadly correspond to those of the Health and Safety at Work Act 1974.

79 The Nuclear Industries Security (Amendment) Regulations 2006 Statutory Instrument 2006 No. 2815.

- These regulations amend the Nuclear Industries Security Regulations 2003
- The principal amendment of these Regulations is to amend Regulation 22 of NISR2003. The amended Regulation 22 provides that the people to whom the regulation applies must maintain appropriate security standards to minimise risk of loss, theft or unauthorised disclosure of sensitive nuclear information.

80 NISR2003, Technical Requirements Document – Minimum Standards for the Physical Protection of Civil Licensed Nuclear sites. Other Nuclear Premises and Nuclear Material in Transit.

- This document was issued by OCNS to support implementation of the NISR2003.
- Part Seven (Ref. 6) of this document details the security objectives, requirements and model standards for a New Nuclear Power Station.

81 CWP/G8 - Classification Policy – Information concerning the Use, Storage and Transport of Nuclear and Other Radioactive Material (Ref. 7).

- This policy document was issued by OCNS to support implementation of the NISR2003.

- The purpose of this policy is to indicate those categories of Protectively Marked Information (PMI) that require protection and the level of protective marking to be applied.
- CWP/G8 deals with the protective marking of information, including that held on IT systems, relating to nuclear facilities, VAs, NM and ORM (including radioactive sources) and material designated as waste.
- In the interests of national security, a particular objective of this policy is to prevent the disclosure of information which could assist those planning a terrorist act, theft, sabotage or other malicious acts (see also paragraph 6).
- Its application is therefore an integral element in the security of nuclear facilities (existing and proposed), NM and ORM.

82 Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities - INFCIRC/225/Revision 5 (Ref. 11).

- This document was issued by the International Atomic Energy Agency (IAEA).
- It is designed to assist Member States to put into practice a comprehensive physical protection regime, against malicious acts, for nuclear facilities and NM.
- It contains a set of recommended requirements to achieve the four physical protection objectives[7] and to apply the twelve fundamental principles[8] that were endorsed by the IAEA Board of the Governors and General Conference.
- Fundamental Principles G, H, I and L (see footnotes 1, 4, 5 and 3 above) have been addressed in the GDA assessment.

[7] To protect against unauthorised removal; To locate and recover missing nuclear material; To protect against sabotage; and To mitigate or minimize effects of sabotage.

[8] Fundamental Principle A: Responsibility of the State
Fundamental Principle B: Responsibilities during International Transport
Fundamental Principle C: Legislative and Regulatory Framework
Fundamental Principle D: Competent Authority
Fundamental Principle E: Responsibility of the Licence Holders
Fundamental Principle F: Security Culture
Fundamental Principle G: Threat
Fundamental Principle H: Graded Approach
Fundamental Principle I: Defence in Depth
Fundamental Principle J: Quality Assurance
Fundamental Principle K: Contingency Plans
Fundamental Principle L: Confidentiality

5 CONCLUSIONS

83 This report presents the findings of the Step 4 Security Assessment of the Westinghouse AP1000 reactor.

84 To conclude, ONR (CNS) are broadly satisfied with the claims, arguments and evidence laid down within the documentation (Refs 14, 15, 16, 17, 18 and 19) relating to VAI and the CSA document (Ref. 29) and supporting documentation. ONR (CNS) considers that from a security viewpoint, the Westinghouse AP1000 generic design will be suitable for construction in the UK, subject to satisfactory resolution of ONR (CNS) findings to date.

85 It is possible that a SSC not considered vital in the generic design would need to be re-designated as such, when built at a future site. Therefore, respective Site Licensees will need to carry out their VAI review against the extant NIMCA document, to determine if site specific decisions have made any impact on the list of potential VAs.

86 The CSA is not intended to detail the specific choice of equipment and technology for plant and systems for a future new build. Turnstiles, automatic access control, intruder detection systems closed circuit television equipment and other security technology is continually evolving to counter a changing threat. Therefore it will be for the Site Licensee to agree with the Security Regulator the specific equipment requirements to meet the prevailing security objectives.

87 These conclusions are subject to the satisfactory progression and resolution of GDA findings to be addressed during site licensing. This includes the assessment of additional information that becomes available as the GDA Design Reference is developed or supplemented with additional details that effect security.

5.1 Key Findings from the Step 4 Assessment

88 The assessment of the AP1000 has concentrated on four main areas; Vital Area Identification (VAI), the identification of the physical locations of the CBSIS, the identification of the existing security arrangements in the generic design and the validation of Westinghouse's CSA.

89 The potential Vital Areas have been adequately identified.

90 The physical location of CBSIS has been as fully identified as practicable in GDA and their protection is covered in the CSA.

91 The existing security arrangements in the generic design have been assessed and deemed acceptable.

92 The Westinghouse CSA (Ref. 29) has been assessed and deemed acceptable.

5.1.1 Assessment Findings

93 ONR (CNS) conclude that the following Assessment Findings listed in Annex 1, including actions for Westinghouse and Site Licensees, should be programmed during the forward programme of this reactor as normal regulatory business.

5.1.2 GDA Issues

94 ONR (CNS) concludes that there are no GDA Issues from this Security Assessment.

6 REFERENCES

1 *Guidance Document for Generic Design Assessment Activities*. Version 2 201206. Office for Civil Nuclear Security. January 2007. www.hse.gov.uk/nuclear/ocns/ocnsdesign.pdf.

2 *GDA Step 4 Security Assessment Plan for the Westinghouse AP1000*. HSE-ND Assessment Plan AR 09/072. April 2010. TRIM Ref. 2010/62497.

3 *Step 3 Security Assessment of the Westinghouse AP1000*. HSE-ND Assessment Report AR 09/042. October 2009. TRIM Ref. 2009/405546.

4 *Guidance to Requesting Parties for Developing the Conceptual Security Arrangements*. Letter from ND to AP1000 Project Front Office. WEC70144R. 3 February 2010. TRIM Ref. 2010/58162.

5 *Nuclear Industries Malicious Capabilities Planning Assumptions*. Office for Civil Nuclear Security. 27 June 2008. File Ref. SB5/2/4/3.

6 *Technical Requirements Document, Part Seven*. Office for Civil Nuclear Security, February 2010. TRIM Ref. 2010/61240.

7 *Classification Policy – Information concerning the Use, Storage and Transport of Nuclear and Other Radioactive Material*. Office for Civil Nuclear Security. GWP/G8, October 2009. Trim Ref. 2009/427676.

8 *Security Policy Framework, Civil Nuclear Security Standard No 2, Protective Marking and Asset Control*. Office for Civil Nuclear Security. Issue 1, June 2010. TRIM Ref. 2010/242242.

9 *Anti-terrorism, Crime and Security Act 2001 (c24).* The Stationary Office (TSO). December 2001.

10 *The Physical Protection of Nuclear Material and Nuclear Facilities*. International Atomic Energy Agency. INFCIRC/225/Revision 4. June 1999.

11 *Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities*. International Atomic Energy Agency. INFCIRC/225/Revision 5. January 2011.

12 *Westinghouse – Comments on Draft Conceptual Security Arrangements Document*. HSE-ND. Letter WEC70275R, 15 December 2010. TRIM Ref. 2010/619700.

13 *Step 4 Security Technical Assessment of the Westinghouse AP1000® Reactor*. HSE-ND. Draft. 31 March 2011. TRIM Ref. 2011/195173.

14 *AP1000 Safeguards Assessment.* Westinghouse. APP-GW-GLR-066 Revision 1. August 2007. File Ref. SB5/18/10/9.

15 *AP1000 Safeguards Assessment.* Westinghouse. APP-GW-GLR-066, Revision 2, November 2008. File Ref. SB5/18/10/9.

16 *AP1000 Safeguards Assessment*. Westinghouse. APP-GW-GLR-066, Revision 4, May 2010. File Ref. SB5/18/10/9.

17 *AP1000 Safeguards Assessment*. Westinghouse. APP-GW-GLR-066, Revision 5, July 2010. File Ref. SB5/18/10/9.

18 *AP1000 Enhancement Report*. Westinghouse. APP-GW-GLR-062, Revision 1, March 2007. File Ref. SB5/18/10/9.

19 *AP1000 Vital Equipment List*. Westinghouse. APP-SES-M3C-001, Revision 1, October 2009. File Ref. SB5/18/10/9.

20 *AP1000 Technical Report Review*. Westinghouse. RAI-TR94-NSIR-34 Supplemental 1. File Ref. SB5/18/10/9.

21 *AP1000 Technical Report Review*. Westinghouse. RAI-TR94-NSIR-28 Supplemental 02a. File Ref. SB5/18/10/9.

22 *AP1000 UK Conceptual Security Plan*. Westinghouse. UKP-GW-GLR-019, Revision A, November 2010. File Ref. SB5/18/10/9.

23 *AP1000 UK Conceptual Security Plan*. Westinghouse. UKP-GW-GLR-019, Revision B, November 2010. File Ref. SB5/18/10/9.

24 *AP1000 Cyber Security Design Criteria*. APP-GW-E1-006 Revision 0. Westinghouse Electric Company LLC. August 2009. TRIM Ref. 2011/93477.

25 *AP1000 Cyber Security Implementation*. APP-GW-GLR-104 Revision 0. Westinghouse Electric Company LLC. May 2007. TRIM Ref. 2008/90845.

26 *AP1000 Nuclear Plant Project Control for Safeguards Information*. APP-GW-GAP-300 Revision 4. Westinghouse Electric Company LLC. January 2008. File Ref. SB5/18/10/9.

27 *Response to RO75*. Westinghouse Letter DCP-JNE-000258. UN REG WEC 00264. 12 July 2010. TRIM Ref. 2010/307817.

28 *Westinghouse – Vital Area Identification*. ONR internal letter. 3 May 2011. TRIM Ref. 2011/130999.

29 *AP1000 UK Conceptual Security Plan*. Westinghouse. UKP-GW-GLR-019, Revision C, June 2011. File Ref. SB5/18/10/9.

30 *Step 4 Radioactive Waste and Decommissioning Assessment of the Westinghouse AP1000® Reactor*. ONR Assessment Report ONR-GDA-AR-11-014, Revision 0. TRIM Ref. 2010/581517.

31 *Step 4 Civil Engineering and External Hazards Assessment of the Westinghouse AP1000® Reactor*. ONR Assessment Report ONR-GDA-AR-11-002, Revision 0. TRIM Ref. 2010/581528.

32 *Step 4 Control and Instrumentation Assessment of the Westinghouse AP1000® Reactor*. ONR Assessment Report ONR-GDA-AR-11-006, Revision 0. TRIM Ref. 2010/581525.

33 *Department of Energy and Climate Change (DECC) Fact Sheet 10.* Available via www.decc.gov.uk.

Table 1

GDA Supporting Documentation for Security Sampled During Step 4

GDA Supporting Documentation Title / Ref.	Section / Area Relevant to this Report
APP-GW-GLR-066 AP1000 Safeguards Assessment	Describes the physical protection system and analyses the ability to provide protection against radiological sabotage.
APP-GW-GLR-062 AP1000 Enhancement Report	Summarises enhancements to the AP1000 design that contributes to the development of a comprehensive physical security programme.
APP-SES-M3C-001 AP1000 Vital Equipment List	List of AP1000 Vital Equipment.
UKP-GW-GLR-019 AP1000 UK Conceptual Security Arrangements	Conceptual Security Arrangements.

Table 2

Relevant Security Policy Documents Considered During Step 4

No.	Title	Description
1	Nuclear Industries Security Regulations 2003	Regulations.
2	NISR2003 - Technical Requirements: Minimum Standards for The Physical Protection of Civil Licensed Nuclear Sites, Other Nuclear Premises and Nuclear Material In Transit	Document containing the security objectives, requirements and model standards for civil nuclear establishments.
3	Nuclear Industries Malicious Capabilities Planning Assumptions	Document detailing the UK threat.
4	CWP/G8 – Classification Policy – Information concerning the use, storage and transport of nuclear and other radioactive material	Classification policy to determine the appropriate protective marking of information.
5	The Physical Protection of Nuclear Material and Nuclear Facilities - INFCIRC/225/Revision 4	International recommendations and requirements for physical protection against sabotage of nuclear facilities and nuclear material during use and storage.
6	Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities - INFCIRC/225/Revision 5	International recommendations and requirements for physical protection against sabotage of nuclear facilities and nuclear material during use and storage.

Annex 1

Assessment Findings to Be Addressed During the Forward Programme as Normal Regulatory Business

Security – AP1000

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-AP1000-SEC-01	The Site Licensee are to demonstrate that generic security features are unaffected by site specific arrangements.	First structural concrete
AF-AP1000-SEC-02	The Site Licensee should make themselves aware of the security objectives and requirements in the extant Technical Requirements Document, Part Seven, or any replacement.	First structural concrete
AF-AP1000-SEC-03	Site Licensee will need to address site specific issues, such as the location of the Security Force Control Centre, while developing the Construction Security Plan and site layout.	First structural concrete
AF-AP1000-SEC-04	The Site Licensee will need to carry out their own Vital Area Identification process taking into account the extent of the relevant malicious capabilities in NIMCA that need to be considered to validate the Westinghouse VA list and confirm that no VAs are created for the site specific application of the AP1000 technology not identified in GDA.	First structural concrete
AF-AP1000-SEC-05	The Site Licensee will need to demonstrate that the Technical Security Systems design(s) will meet the requirements of TRD.	Install RPV
AF-AP1000-SEC-06	The Site Licensee will need to engineer long term power supply to support the security infrastructure and demonstrate its adequacy.	Install RPV
AF-AP1000-SEC-07	Not used	
AF-AP1000-SEC-08	The Site Licensee will need to carry out a vulnerability assessment for their proposed site layout and security force staffing to confirm and demonstrate that the measures in the CSA continue to meet the security objectives in TRD Part Seven.	Nuclear island safety related concrete

Annex 1

Assessment Findings to Be Addressed During the Forward Programme as Normal Regulatory Business

Security – AP1000

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-AP1000-SEC-09	The Site Licensee will need to confirm and provide evidence that the security doors to be installed meet the requirements of TRD.	Install RPV
AF-AP1000-SEC-10	The Site Licensee will need to determine the specific AACS equipment that will be needed to meet the requirements in TRD	Install RPV
AF-AP1000-SEC-11	The Site Licensee will need to ensure that searching requirements in TRD Part Seven can be fulfilled.	Install RPV
AF-AP1000-SEC-12	The Site Licensee will need to develop procedures to meet the security objectives for access to the Containment Building under all plant conditions.	Fuel on-site
AF-AP1000-SEC-13	The Site Licensee will need to determine that the emergency routes confirm to UK requirements and ensure that security measures are not compromised.	Nuclear island safety related concrete
AF-AP1000-SEC-14	The Site Licensee will need to protect CBSIS against cyber attack, manipulation and falsification to the appropriate Information Security standards as determined by ONR (CNS).	Mechanical, Electrical and C&I Safety Systems – Before delivery to Site

Note: It is the responsibility of the Licensees / Operators to have adequate arrangements to address the Assessment Findings. Future Licensees / Operators can adopt alternative means to those indicated in the findings which give an equivalent level of security.

For Assessment Findings relevant to the operational phase of the reactor, the Licensees / Operators must adequately address the findings during the operational phase. For other Assessment Findings, it is the regulators' expectation that the findings are adequately addressed no later than the milestones indicated above.

Annex 2

GDA Issues – Security – AP1000

There are no GDA Issues for this topic area.