Office for Nuclear Regulation

An agency of HSE

Generic Design Assessment – New Civil Reactor Build

Step 4 Security Assessment of the EDF and AREVA UK EPR™ Reactor

Assessment Report: ONR-GDA-AR-11-031
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 EDF and AREVA relating to the UK EPR™ 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 EDF and AREVA 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 EDF and AREVA UK EPR™ reactor.

EXECUTIVE SUMMARY

This report presents the findings of the Security Assessment of the EDF and AREVA UK EPR 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 EDF and AREVA during Step 4.

This assessment followed a step-wise-approach in a claims-argument-evidence hierarchy. In Step 2 the claims made by EDF and AREVA 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 UK EPR reactor in greater detail, by examining the evidence, supporting arguments and claims made in the submitted 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 has focussed on:

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

A number of items have been agreed with EDF and AREVA 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 present an adequate security case for the generic UK EPR reactor design. The UK EPR 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 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 UK EPR have material changes made to the design.

The security measures for the generic elements of the UK EPR 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 EDF and AREVA 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
EDF and AREVA	Electricité de France SA and AREVA NP SAS
EPR	European Pressurised-water Reactor
ERL	Emergency Reference Level
GDA	Generic Design Assessment
GSA	General Security Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the French Republic concerning the Mutual Protection of Classified Information, CM7425
HSA	High Security Area
HSE	The Health and Safety Executive
IAEA	The International Atomic Energy Agency
I & A	Integrity and Availability
ILW	Intermediate Level Waste
MEEDM	Ministère de L'Écologie, de L'Énergie, du Développement Durable et de la Mer
MEDDTL	Ministère de L'Écologie, du Développement Durable, des Transports et du Logement
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
PMI	Protectively Marked Information
PCER	Pre-construction Environmental Report
PCSR	Pre-construction Safety Report
PSA	Probabilistic Safety Analysis
SAP	Safety Assessment Principles

LIST OF ABBREVIATIONS

SSC	System, Structure and Component
TQ	Technical Query
TRD	Technical Requirements Document
TSC	Technical Support Contractor
VA	Vital Area
VAI	Vital Area Identification
VASB	Vital Area Security Barrier

TABLE OF CONTENTS

Tables

Annexes

Annex 1: Assessment Findings to be Addressed During the Forward Programme as Normal Regulatory Business - Security – UK EPR

Annex 2: GDA Issues - Security – UK EPR

1 INTRODUCTION

1 This report presents the Security Assessment findings for the EDF and AREVA UK EPR 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 EDF and AREVA (Ref. 4). This report concentrates mainly on the Vital Area Identification (VAI), Computer Based Systems Important to Nuclear Safety (CBSIS) and Conceptual Security Arrangements (CSA) for the UK EPR reactor, and the supporting documentation provided by EDF and AREVA under the Office for Nuclear Regulation (ONR) Generic Design Assessment (GDA) process.

2 The assessment took into account the UK EPR Physical Protection report (Ref. 14) that contains details of the VAI for the UK EPR and supporting documents (Refs 15, 17, 18 and 19), and the submitted versions of the CSA (Refs 16, 20 and 23). The approach taken was to review the submissions, and then 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 EDF and AREVA by letter on several occasions requesting additional information. Periodic meetings were also held between OCNS and EDF and AREVA to promote understanding, discuss progress and agree the next steps. The Technical Queries (TQ) process was not used during the GDA 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 have been agreed with EDF and AREVA 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. 25).

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

marked information (PMI), originated by the United Kingdom or the Republic of France. 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 a UK EPR 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 plans concentrated on 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 EDF and AREVA's CSA.

9 VAI ties in with the graded approach[4] to radiological consequences of 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 holding Nuclear Material (NM) or Other Radioactive Materials (ORM), or any other identified Vital Area (VA), in such a manner as to create a serious 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 (SSCs) comprising part of the site's infrastructure could create (without appropriate security measures in place) a radiological hazard to the public and/or environment. At such sites, the potential for sabotage and the associated potential radiological consequences are 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 Vital Areas (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 EDF and AREVA, 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 control system that maintains working parameters within pre-defined limits by responding continuously to normal plant operations).

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

12 The Control and Instrumentation (C&I) assessment (Ref. 27) 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 EDF and AREVA 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) are also detailed.

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 topics and detailed in Step 4 Assessment Report ONR-GDA-AR-11-018 (Ref. 26). The transfer and control of Protectively Marked Information (PMI) between EDF and AREVA 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 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-UKEPR-SEC-13**).

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

AF-UKEPR-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 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 given in the CSA guidance document sent to EDF and AREVA with letter EPR70152R dated 3 February 2010 (Ref. 4).

20 The identification of the CBSIS systems was carried out by the RP and validated by the ND Safety Assessor for Control and Instrumentation (C&I). The standards and criteria are detailed in the C&I Step 4 Assessment Report (Ref. 27).

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 (SAP) (Ref. 24) 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 RP 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 and its subsequent revisions were 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, Ref. 28).

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 System, Structure and Component (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.

External Hazards

- Aircraft impact.
- Explosion and the effect of blast.

Internal Hazards

- Fire.
- Flooding.
- Internal missiles generated through plant failures.

Control and Instrumentation

- Computer Based Systems Important to Nuclear Safety (CBSIS).

Probabilistic Safety Analysis

- Multiple failures and the resulting consequences.

Fault Studies

- Individual and multiple failures and the resulting consequences.

Civil Engineering

- Robustness of building structures.

2.3.6 Out of Scope Items

27 The following items have been agreed with the RP 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 EDF AND AREVA'S SECURITY SUBMISSIONS

3.1 EDF and AREVA's Vital Area Identification

28 The VAI document (Ref. 14) and the design of doors document (Ref. 15) both protectively marked CONFIDENTIEL DEFENSE, treated as equivalent to UK CONFIDENTIAL, were supplied directly to OCNS through the General Security Agreement (GSA) (Ref. 21) between the UK and France.

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

30 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 in Ref. 22.

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

32 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 EDF and AREVA's Computer Based System Important to Safety

33 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.

34 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-UKEPR-SEC-014**).

> **AF-UKEPR-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.

35 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 EDF and AREVA's Conceptual Security Arrangements

36 The submitted Conceptual Security Arrangements (CSA) document (Refs 16, 20 and 23) are protectively marked, were supplied to OCNS through the General Security Agreement (Ref. 21) between the UK and France and contain sections on:

- Vital Area Identification methodology;
- The Vital Areas;
- The physical protection, including the Vital Area Security Barrier (VASB), afforded to those Vital Area systems, structures and components (SSC);
- The Computer Based Systems Important to Nuclear Safety (CBSIS);
- Access control into and around the nuclear island and Vital Areas; and
- Associated drawings and tables.

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

38 Guidance on the content and layout of the Conceptual Security Arrangements document was sent to EDF and AREVA in letter EPR70152R dated 3 February 2010 (Ref. 4). Subsequent meetings have been undertaken to support the RP's development of the CSA document for the UK EPR.

39 Comments on Issue 1 of the CSA (Ref. 16) are contained in EPR70268R dated 18 November 2010 (Ref. 12).

4 GDA STEP 4 NUCLEAR DIRECTORATE ASSESSMENT FOR SECURITY

4.1 Vital Area Identification

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

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

4.1.1 Assessment

42 The report (Ref. 14) substantially reproduced in Issue 2 of the CSA document (Ref. 20), which was submitted identifying the VAs in the UK EPR 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 vital areas.

4.1.2 Findings

43 The VAI report (Ref. 14) categorised SSCs into three groupings; 'At-risk', 'Critical' and 'Vital'; and introduced the term 'Nevralgic' that had been used during the design stage to differentiate between the vulnerability of Vas. This refinement is unnecessary for the VAI as the primary purpose is the identification of VAs irrespective of the vulnerability or otherwise to allow the appropriate security to be developed deterministically.

44 During the assessment, security and safety assessors working together, decided that several of the SSCs identified as 'Critical' should, for the purposes of the CSA and the GDA assessment, be re-categorised as 'Vital'. This decision was given at a meeting in October 2010 to the RP that was attended by OCNS and ONR Safety colleagues, from both GDA and SINS. This change was effected in Issue 3 of the CSA document (Ref. 23)

45 The assessment has confirmed that the site specific VAI should lead to the decision on whether potential vital areas are actual VAs or not. It has also confirmed that it is easier to postulate that a SSC is 'Vital' than it is to present arguments and evidence why a SSC is 'not-vital'.

46 The RP carried out their assessment without being in possession of the 'UK Eyes Only' 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, is still effective in identifying the significant SSCs that could lead to unacceptable radiological consequences.

4.2 Computer Based Systems Important to Nuclear Safety

47 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.

48 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 33) will be determined during Site Licensing and construction.

4.2.1 Assessment

49 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

50 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.

51 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

52 The completed CSA document for the UK EPR is to detail:

- the locations of the potential VAs requiring protection;
- identify the proposed physical security protection measures for those VAs including the Vital Area Security Barrier (VASB);
- the access control measures for the nuclear island and the VAs; and
- the same information for CBSIS.

53 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

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

4.3.2 Findings

55 The detailed findings and actions on Issue 2 of the CSA document (Ref. 20) are in Revision A of the protectively marked technical report at Ref. 13.

56 Issue 3 of the CSA (Ref. 23) took account of the findings in Revision A of Ref. 13. Issue 3 has been assessed by ONR (CNS) and is deemed to provide a robust and acceptable submission that meets the regulatory requirements.

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

58 Vital Area Identification (VAI)

- Acknowledgement is made within the CSA that any Potential Licensee 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 GDA (Assessment Finding **AF-UKEPR-SEC-04**).

  AF-UKEPR-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 RP VA list and confirm that no VAs are created for the site specific application of the UK EPR 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.

59 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-UKEPR-SEC-14**) (See paragraph 34).

60 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 OCNS assessment.
- Specific equipment for access control and associated operating procedures will be determined through interaction with Potential Licensees (Assessment Finding **AF-UKEPR-SEC-10**).

  AF-UKEPR-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.

61 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-UKEPR-SEC-02** and **AF-UKEPR-SEC-09**).

  AF-UKEPR-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-UKEPR-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.

62 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-UKEPR-SEC-05** and **AF-UKEPR-SEC-10**).

  AF-UKEPR-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-UKEPR-SEC-10: *See paragraph 60.*

- The location of the Security facilities 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-UKEPR-SEC-03**).

  AF-UKEPR-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-UKEPR-SEC-06**).

  AF-UKEPR-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.

63 Site Specific Buildings

- Aspects of site specific buildings, such as the interconnections between the nuclear island and the Turbine Hall, should not compromise the generic security arrangements (Assessment Finding **AF-UKEPR-SEC-01**).

  AF-UKEPR-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.

64 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-UKEPR-SEC-08**).

  AF-UKEPR-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-UKEPR-SEC-11**).

  AF-UKEPR-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-UKEPR-SEC-12**).

  AF-UKEPR-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

65 OCNS have been working effectively with the French Competent Authority, Ministère de L'Écologie, de L'Énergie, du Développement Durable et de la Mer (MEEDM), now Ministère de L'Écologie, du Développement Durable, des Transports et du Logement (MEDDTL), in managing the transfer of classified information between HSE ND and EDF and AREVA using the GSA (Ref. 21). Although some delays occurred in the time taken for documents to be transferred the process has, in the main, been effective.

66 Both Regulators have also been effective in managing security clearance lists for those accessing protectively marked information (PMI) passed through the GSA.

4.5 Multilateral Collaboration

67 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

68 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.

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

4.7 Other Relevant Legislation and Guidance

70 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.

71 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.

72 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 7 (Ref. 6) of this document details the security objectives, requirements and model standards for a New Nuclear Power Station.

73 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 above).
- Its application is therefore an integral element in the security of nuclear facilities (existing and proposed), NM and ORM.

74 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) 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

75 This report presents the findings of the Step 4 Security Assessment of the EDF and AREVA UK EPR reactor.

76 To conclude, ONR (CNS) is broadly satisfied with the claims, arguments and evidence laid down within the document (Ref. 14) relating to VAI and the CSA document (Ref. 23). ONR (CNS) consider that from a security viewpoint, the EDF and AREVA UK EPR generic design will be suitable for construction in the UK, subject to satisfactory resolution of ONR (CNS) findings to date.

77 As the RP carried out their vital area assessment without being in possession of the 'UK Eyes Only' NIMCA document 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. Nevertheless, 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, particularly for SSCs not covered in GDA. The 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.

78 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.

79 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

80 The assessment of the UK EPR 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 EDF and AREVA's CSA.

81 The potential Vital Areas have been adequately identified.

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

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

84 The RP CSA (Ref. 23) has been assessed and deemed acceptable.

5.1.1 Assessment Findings

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

5.1.2 GDA Issues

86 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 EDF and AREVA UK EPR*. HSE-ND Assessment Plan AR 09/071. April 2010. TRIM Ref. 2010/62503.

3 *Step 3 Security Assessment of the EDF and AREVA UK EPR*. HSE-ND Assessment Report AR 09/043, October 2009. TRIM Ref. 2009/405549.

4 *Guidance to Requesting Parties for Developing the Conceptual Security Arrangements.* HSE-ND. Letter EPR70152R. 3 February 2010. TRIM Ref. 2010/56953

5 *Nuclear Industries Malicious Capabilities Planning Assumptions*. OCNS. 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 *EDF and AREVA - Conceptual Security Arrangements draft document – feedback*. HSE-ND. Letter EPR70268R, 18 November 2010.

13 *Step 4 Security Technical Assessment of the EDF and AREVA UK EPR™*. ONR, Draft 18 March 2011. Trim Ref. 2011/157050.

14 *UK EPR Physical Protection Principle*. EDF. July 2009. File Ref. SB5/18/10/8.

15 *Design of EPR Doors*. EDF. July 2010. File Ref. SB5/18/10/8.

16 *UK EPR Conceptual Security Arrangements*. EDF and AREVA. Issue 01. September 2010. File Ref. SB5/18/10/8.

17 *EPR – Nuclear Island Evacuation Drawings*. EDF. January 2011. File Ref. SB5/18/10/8.

18 *Security Barrier Specification for UK EPR Power Plants*. EDF. December 2010. File Ref. SB5/18/10/8.

19 *CSA update – Drawings. Letter from UK EPR Project Front Office to ND*. 14 February 2010. File Ref. SB5/18/10/8.

20 *UK EPR Conceptual Security Arrangements*. EDF and AREVA. Issue 02. January 2011. File Ref. SB5/18/10/8.

21 *Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the French Republic concerning the Mutual Protection of Classified Information*. CM7425. France No.1. TSO (The Stationary Office). 2008. File Ref. SB5/18/10/8.

22 *EDF and AREVA – Vital Area Identification. ONR internal letter*. 3 May 2011. TRIM Ref. 2011/130917.

23 *UK EPR Conceptual Security Arrangements*. EDF and AREVA. Issue 03. June 2011. File Ref. SB5/18/10/8.

24 *Safety Assessment Principles for Nuclear Facilities.* 2006 Edition Revision 1. HSE. January 2008. www.hse.gov.uk/nuclear/saps/saps2006.pdf.

25 *Step 4 Radioactive Waste and Decommissioning Assessment of the EDF and AREVA UK EPR™ Reactor*. ONR Assessment Report ONR-GDA-AR-11-030 Revision 0. TRIM Ref. 2010/581501.

26 *Step 4 Civil Engineering and External Hazards Assessment of the EDF and AREVA UK EPR™ Reactor*. ONR Assessment Report ONR-GDA-AR-11-018 Revision 0. TRIM Ref. 2010/581513.

27 *Step 4 Control and Instrumentation Assessment of the EDF and AREVA UK EPR™ Reactor*. ONR Assessment Report ONR-GDA-AR-11-022 Revision 0. TRIM Ref. 2010/581510.

28 *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
UK EPR Physical Protection Principle	Details the Vital Area Identification methodology and those Systems, Structures and Components that are considered 'At risk', 'Critical' and 'Vital'
[redacted] - Design of EPR doors	Identifies locations and type of security doors
Conceptual Security Arrangements Issue 01	Conceptual Security Arrangements
Conceptual Security Arrangements Issue 02	Conceptual Security Arrangements
Conceptual Security Arrangements Issue 03	Conceptual Security Arrangements
EPR – Nuclear Island Evacuation Drawings	Drawings identifying egress routes
ND(OCNS) EPR00757N	Drawings of Reactor Building Access Airlock and equipment hatch Drawings of removable walls
Security Barrier Specification for UK EPR Power Plants	Requirements applicable to UK EPR openings
Revision I1 List of doors and openings	Data and drawings concerning certain doors and openings on the UK EPR

Table 2

Relevant Security 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
7	General Security Agreement (GSA) between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the French Republic concerning the Mutual Protection of Classified Information CM7425	Agreement for managing the transfer of protectively marked information between France and UK

Annex 1

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

Security – UK EPR

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-UKEPR-SEC-01	The site licensee are to demonstrate that generic security features are unaffected by site specific arrangements.	First structural concrete
AF-UKEPR-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-UKEPR-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-UKEPR-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 RP VA list and confirm that no VAs are created for the site specific application of the UK EPR technology not identified in GDA.	First structural concrete
AF-UKEPR-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-UKEPR-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-UKEPR-SEC-07	Not Used	

Annex 1

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

Security – UK EPR

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-UKEPR-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
AF-UKEPR-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-UKEPR-SEC-010	The site licensee will need to determine the specific AACS equipment that will be needed to meet the requirements in TRD	Install RPV
AF-UKEPR-SEC-011	The site licensee will need to ensure that searching requirements in TRD Part Seven can be fulfilled.	Install RPV
AF-UKEPR-SEC-012	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-UKEPR-SEC-013	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-UKEPR-SEC-014	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

Annex 1

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 – UK EPR

There are no GDA Issues for this topic area.