



ONR GUIDE			
GUIDANCE ON THE SECURITY ASSESSMENT OF GENERIC NEW NUCLEAR REACTOR DESIGNS			
Document Type:	Nuclear Security Technical Assessment Guide		
Unique Document ID and Revision No:	CNS-TAST-GD-007 Revision 0		
Date Issued:	May 2014	Review Date:	May 2017
Approved by:	Brett Roberts-Howe	Superintending Inspector	
Record Reference:	TRIM Folder 1.9.3.740. (2014/0173946)		
Revision commentary:	New document issued		

TABLE OF CONTENTS

1. INTRODUCTION	2
2. PURPOSE AND SCOPE	2
3. RELATIONSHIP TO LICENCE AND OTHER RELEVANT LEGISLATION	2
4. RELATIONSHIP TO SAPS, WENRA REFERENCE LEVELS AND IAEA SAFETY STANDARDS ADDRESSED	3
5. ADVICE TO INSPECTORS	3
6. VITAL AREA IDENTIFICATION	4
7. CONCEPTUAL SECURITY ARRANGEMENTS	4
8. KEY FEATURES OF A CONCEPTUAL SECURITY ARRANGEMENTS SUBMISSION	4
9. REPORTING ASSESSMENT FINDINGS	6
10. REFERENCES	7
11. GLOSSARY AND ABBREVIATIONS	8

1. INTRODUCTION

- 1.1 The Office for Nuclear Regulation (ONR) has established its security objectives for dutyholders to meet. The security regime for meeting these objectives is described in the Nuclear Site Security Plans (NSSPs) prepared by dutyholders, which are approved by ONR. These objectives are given in the National Objectives, Requirements and Model Standards (NORMS) document, which describes how the objectives might be achieved through a set of requirements and model standards. Other security arrangements may be applied provided they meet the objectives. NORMS is supported by a suite of guides to assist ONR inspectors in their assessment and inspection work, and in making regulatory judgements and decisions. This Technical Assessment Guide (TAG) is such a guide.

2. PURPOSE AND SCOPE

- 2.1 This TAG contains guidance to advise and inform Security Inspectors in the Office for Nuclear Regulation (ONR) in exercising of their regulatory judgement. It aims to provide general advice and guidance to ONR Security Inspectors on how to assess the adequacy of generic designs for nuclear reactor facilities.
- 2.2 The Generic Design Assessment (GDA) (Reference 1) process requires the Requesting Party (RP) to submit sufficient information to enable the Regulator to make an informed judgement of the adequacy of the security aspects of the generic design, to support the construction and subsequent operation of this technology in the UK.
- 2.3 Generic designs do not address some of the site specific elements which will influence the security infrastructure required at a particular site. This may include the need for technology at a multi-unit site, which supports common access arrangements throughout the site, and other common services (e.g. the location and nature of security specific assets).
- 2.4 GDA process also gives confidence to the RP that the assessed security aspects of the design, when subsequently applied at a specific site, will meet ONR's regulatory expectation.

3. RELATIONSHIP TO LICENCE AND OTHER RELEVANT LEGISLATION

- 3.1 The GDA process sits outside the formal ONR regulation regime and vires. It is, therefore, undertaken on a voluntary basis by the RP through a contractual arrangement with ONR to allow for cost recovery.
- 3.2 The GDA process involves the production, exchange and review of Sensitive Nuclear Information (SNI). Those who handle SNI as part of this process are subject to Regulation 22 of the Nuclear Industries Security Regulations 2003 (NISR 2003) (References 2, 3 and 4). They should also comply with the Security Policy Framework (SPF) (see paragraph **Error! Reference source not found.**) (Reference 9). The ONR assessment should ensure that appropriate arrangements are put in place by all parties to manage and protect any SNI wherever it is held. This includes the wider ONR organisation and the Technical Support Contractors (TSC) who are employed to assist the assessment process. Support from within ONR, specifically from the InfoSec team, should be obtained as necessary to support the assessment and review the management of SNI across the wider project.
- 3.3 The ONR Security Inspector(s) should also consider the need for individuals within the RP or the contracted organisations to hold appropriate security clearances.

- 3.4 There may be a General Security Agreement (GSA) between the United Kingdom and a country where the RP is working on UK SNI or SNI developed by the RP. Transfer of the SNI between these countries must, therefore, comply with the GSA.

4. RELATIONSHIP TO SAPS, WENRA REFERENCE LEVELS AND IAEA SAFETY STANDARDS ADDRESSED

- 4.1 This TAG is consistent with the principles described in the international and national documents highlighted below.
- 4.2 The IAEA document INFCIRC225 Revision 5 (Reference 5) at paragraphs 3.45 to 3.47.27, supporting Fundamental Principle I: Defence in Depth, details that physical security arrangements require a mixture of hardware, procedures and facility design. It also states that the physical protection functions of detection, delay and response should each have defence in depth and use a graded approach (Fundamental Principle H) to provide appropriate effective protection against insiders and external threats (Fundamental Principle G).
- 4.3 The IAEA technical guidance document Engineering Safety Aspects of the Protection of Nuclear Power Plants against Sabotage (Reference 6) at section 3.5.1 reviews what constitutes a physical protection system and at section 3.5.2 discusses the need for Vital Area Identification (VAI).
- 4.4 The 'threat assessment/design basis threat' is detailed in the extant version of the Nuclear Industries Malicious Capabilities Planning Assumptions (NIMCA) document (Reference 7).
- 4.5 Part One of the National Objectives, Requirements and Model Standards (NORMS) documents (Reference 8) requires dutyholders to evaluate the potential radiological consequences of sabotage against Nuclear Material (NM), Other Radioactive Materials (ORM) or against specific equipment, systems or devices that form part of a site's infrastructure. The evaluation should identify key assets that prevent unacceptable radiological consequences so they can be designated as VAs and protected by an appropriate physical protection system using a graded approach.
- 4.6 The SPF (Reference 9) is published by the Cabinet Office and is adopted by the whole of the civil nuclear industry for the protection of SNI and the introduction of appropriate personnel security controls whether on and off nuclear premises.
- 4.7 The Classification Policy (Reference 10) indicates those categories of SNI that require protection and the level of protective marking to be applied.

5. ADVICE TO INSPECTORS

- 5.1 The ONR Security Inspector(s) will be required to work as part of a wider regulatory team including other ONR inspectors and staff from the Environment Agency. The ONR Security Inspector will need to consider other Regulatory requirements in making their decisions.
- 5.2 The objective for the security assessment of the generic design is for ONR to judge whether the proposed arrangements will be adequate to meet ONR's regulatory requirements and are likely to be successfully integrated into the overall site arrangements. These would then form a part of the dutyholder's approved Nuclear Site Security Plan (NSSP).

- 5.3 Where there are deficiencies in the submissions or aspects that need further definition or modification at the close of the GDA process these should be recorded as findings. Where these are substantial in scope, quantity or importance they should be recorded as issues. The methodology to record these is found within the wider GDA process definition found in the GDA process on How2.
- 5.4 ONR Security Inspectors are required to make judgements in developing their response to the generic design submission documents. Engagement with the RP(s) is essential to fully understand their proposals and influence the quality and completeness of the final submissions.
- 5.5 The security assessment will need to cover VAI (see section 6) and development of the Conceptual Security Arrangements (CSA) (see section 7) as a minimum.
- 5.6 Evidence to demonstrate that the proposed generic security measures will meet the security objectives identified in NORMS (Reference 8) should be present. The ONR Security Inspector must consider the proposals in the context of application at a UK site and how the generic proposals might be integrated into overall site arrangements. Consideration of multi-unit applications should be factored into this assessment.
- 5.7 The ONR Security Inspector needs to ensure that the final CSA submission from the Requesting Party clearly defines the scope of the plant covered in the CSA. Should the technology described in the CSA be subsequently deployed in the UK then the assessment of the complete design at the site, possibly as a multiple unit installation, the ONR security focus will initially be on those areas not assessed as a part of the CSA work.
- 5.8 It should be remembered that the report produced by ONR Security Inspectors will subsequently be used by a project developer to justify the NSSP for a specific site using such a technology.

6. VITAL AREA IDENTIFICATION

- 6.1 The TAG on the Assessment of Vital Area Identification (Reference 11) should be followed to assess the documents provided by the RP on this subject area.

7. CONCEPTUAL SECURITY ARRANGEMENTS

- 7.1 The CSA document generated by the RP has a number of key deliverables as described in section 8. In essence the CSA must identify the areas requiring protection and the features built into the plant to provide protection to those areas.
- 7.2 The detail available at this time is likely to be conceptual rather than specific, dependant on the level of design development.
- 7.3 The ONR Security Inspector should ensure their activities are integrated with those being undertaken by the ONR Safety Inspectors to help provide a consistent response to the RPs. It is important that the security assessment is integrated into the wider ONR and Environment Agency assessment process to minimise and, as necessary, manage any potentially conflicting requirements.

8. KEY FEATURES OF A CONCEPTUAL SECURITY ARRANGEMENTS SUBMISSION

- 8.1 The CSA document should identify potential Vital Areas (VAs), in line with the UK definition (see NORMS, Part One, Chapter 1, Paragraph 1.1.14 (Reference 8)). It

should also provide details of Computer Based Systems Important to Nuclear Safety (CBSIS) present in the design, including those that may be dependent on specific site features. In addition, the CSA document should identify Computer Based Systems Important to Security (CSISy). The document should contain sufficient technical information on these topics to ensure all relevant issues are clear and readily understood. Drawings and plans should be used to detail where these elements are physically located in the generic design.

- 8.2 The CSA document should include sufficient information on access control arrangements and emergency exits, particularly in areas containing VAs and CBSIS/CSISy, so it is clear how movement into and out of the security zones/areas is controlled. Drawings should identify the location of all external and internal security doors, including those used for emergency purposes, and the features to be installed on these doors e.g. alarms, cameras, and fail safe features. Security ratings should also be identified. Emergency egress routes into and out of secure areas should also be detailed in the document.
- 8.3 The CSA document and associated drawings should detail any security features that will be used, either locally or remotely, to control access to VAs and CBSIS/CSISy. The construction details of the walls, floors or ceilings of areas containing VAs and CBSIS/CSISy, or adjoining such areas, need to be detailed, together with any security features that delay and detect unauthorised intrusion. Security access control arrangements for the different plant states (commissioning, normal operations, maintenance and outage) should also be detailed in the CSA document.
- 8.4 It is reasonable to expect a high level concept of operations to be delivered by the RP which identifies a location or locations where the security system controls and instrumentation (e.g. alarms etc.) will be displayed and monitored. In addition the provision of power to the security infrastructure and associated redundancy, including UPS if necessary, should be set down in the CSA even if plans are at a conceptual level.

Process

- 8.5 The ONR Security Inspector should discuss the above requirements with the RPs and their contractors as necessary, and then request the RP to prepare an outline for the proposed layout and content of the CSA document. ONR will then review the submission and advise the RPs, following discussion if necessary, on the adequacy of the proposed content and layout of the document.
- 8.6 It is expected that the CSA document will include a number of layout drawings. The RPs should check revision numbers of these documents close to the final submission date, to ensure that all the latest information has been included in the submission.
- 8.7 Throughout the GDA process the design will develop, partly as a result of interactions with the Regulators, and new information will be received. It is likely, therefore, that a number of CSA iterations will be received. The ONR Security Inspector(s) must maintain an audit trail that evidences ONR's position and the findings given in GDA reports.
- 8.8 The verification of the RP designated VAs and CBSIS/CSISy will be undertaken by ONR Safety Assessment staff, as part of the GDA process.

Final CSA Submission

- 8.9 The final iteration of the CSA forms part of the RP's GDA submission. It will be reviewed by ONR Security Inspectors and assist with compilation of their technical

assessment report at the end of the GDA process. ONR will make its position clear by approving, rejecting, raising exclusions and/or identifying other actions required by the RP at the end of the process that is consistent with the completion of GDA.

9. REPORTING ASSESSMENT FINDINGS

- 9.1 A reporting format for the GDA assessment reports will be provided to the ONR Security Inspector by the GDA project team. The intention is that all technical assessment reports will be published on the ONR website. Therefore, the ONR Security Inspector should write the report knowing that it will be OFFICIAL, but ensuring it gives as much detail as reasonable given the security classification. It should also describe, openly and transparently, the process followed, the work undertaken and the findings made.
- 9.2 It may be necessary to write an additional technical report at a higher security classification to properly capture all the details, discussions and decisions. This report would not be published on the ONR website, but it would be shared with the RP.

10. REFERENCES

1. **New nuclear power stations - Generic Design Assessment.** A guide to the regulatory processes
2. **Nuclear Industries Security Regulations 2003.** Statutory Instrument 2003 No. 403
3. **Nuclear Industries Security (Amendment) Regulations 2006.** Statutory Instrument 2006 No. 2815
4. **Nuclear Industries Security (Amendment) Regulations 2013.** Statutory Instrument 2013 No. 190
5. IAEA Nuclear Security Series No. 13. Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (**INFCIRC/225/Revision 5**). January 2011. www-pub.iaea.org/MTCD/Publications/PDF/Pub1481_web.pdf.
6. IAEA Nuclear Security Series No. 4. Engineering Safety Aspects of the Protection of Nuclear Power Plants against Sabotage. January 2007. www.iaea.org/books
7. **Nuclear Industries Malicious Capabilities Planning Assumptions.**
8. **National Objectives, Requirements and Model Standards.**
Trim Folder 4.4.2.11304.
9. **HMG Security Policy Framework.** Trim Folder 4.4.2.10457.
10. **Classification Policy – NISR Classification Policy**
11. **Guidance on How to Assess the Adequacy of a Vital Area Identification Submission** - CNS-TAST-GD-005 Revision 0 April 2013 Trim ref: 2012/497668.

Note: ONR staff should access the above internal ONR references via the How2 Business Management System.

11. GLOSSARY AND ABBREVIATIONS

CBSIS	Computer Based Systems Important to Safety
CNS	Civil Nuclear Security
CSA	Conceptual Security Arrangements
CSISy	Computer Systems Important to Security
GDA	Generic Design Assessment
IAEA	International Atomic Energy Agency
NIMCA	Nuclear Industries Malicious Capabilities Planning Assumptions
NISR	Nuclear Industries Security Regulations
NM	Nuclear Material
NORMS	National Objectives, Requirements and Model Standards
NSSP	Nuclear Site Security Plan
ONR	Office for Nuclear Regulation
ORM	Other Radioactive Material
RP	Requesting Party
SNI	Sensitive Nuclear Information
SPF	Security Policy Framework
TAG	Technical Assessment Guide
VAI	Vital Area Identification