Office for Nuclear Regulation

| 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-11.1 Revision 0 | | |
| **Date Issued:** | June 2017 | **Review Date:** | June 2020 |
| **Approved by:** | Dan Hasted | Professional Lead | |
| **Record Reference:** | TRIM Folder 1.1.3.776 2017/203348 | | |
| **Revision commentary:** | New Document Issued | | |

**TABLE OF CONTENTS**




*© Office for Nuclear Regulation, 2017*
If you wish to reuse this information visit www.onr.org.uk/copyright for details.


Published 06/17

## 1. INTRODUCTION

1.1 The Office for Nuclear Regulation (ONR) has established a set of Security Assessment Principles (SyAPs) (Reference 1). This document contains Fundamental Security Principles (FSyPs) that dutyholders must demonstrate have been fully taken into account in developing their security arrangements to meet relevant legal obligations. The security regime for meeting these principles is described in security plans prepared by the dutyholders, which are approved by ONR under the Nuclear Industries Security Regulations 2003 (Reference 2).

1.2 The term 'security plan' is used to cover all security dutyholder submissions such as construction or nuclear site security plans, temporary security plans and transport security statements. The SyAPs are 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 Guidance (TAG) is such a guide.

1.3 Whilst it is the prospective licensee who will develop the site specific security plan, it is expected that a Generic Security Report (GSR) will form the basis of this plan. A GSR, submitted by a Requesting Party (RP) as part of ONR's Generic Design Assessment (GDA), should describe the security features of the technology being assessed. Importantly, it should document the categorisation from both theft and sabotage to determine the protective security outcomes and applicable security postures to be applied. It is therefore important that inspectors carry out their assessment recognising that the security arrangements detailed in the GSR must be able to meet regulatory expectations, in respect of the FSyPs, in order that a future site specific security plan can be approved. In turn, the assessment of the GSR should provide confidence to both the Requesting Party (RP) and potential licensee that the security arrangements for the technology are considered adequate.

## 2. PURPOSE AND SCOPE

2.1 This TAG contains guidance to inform ONR inspectors in exercising their regulatory judgment during assessment activities related to the adequacy of generic designs for new nuclear reactors. It aims to provide general advice and guidance to ONR inspectors on how this aspect of security should be assessed. It does not set out how ONR regulates the dutyholder's arrangements. It does not prescribe the detail, targets or methodologies for dutyholders to follow in demonstrating they have addressed the SyAPs. It is the dutyholder's responsibility to determine and describe this detail and for ONR to assess whether the arrangements are adequate. The GDA Guidance to Requesting Parties (Reference 3) requires the 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 the technology in the UK.

2.2 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 could require common access arrangements throughout the site, and other common services (e.g. the location and nature of security specific assets such as fences or security force locations).

2.3 Defence in depth is a fundamental security principal and the GSR should reflect a concept of several layers and methods of protection (structural, other technical, personnel and organisational). Whilst many of these layers will be determined by the licensee (particularly personnel and organisational), it is important that the physical security arrangements can support the licensee's Concept of Security Operations. Where claims are made on the adequacy of security arrangements which take into

account those measures to be determined by the licensee, for example perimeter fences, gatehouse, hostile vehicle mitigation, personnel security etc, there should be a clear statement articulating how the potential licensee's arrangements are expected to combine with the GSR to mitigate against the threats. This TAG does not prescribe the detail, goals or methodologies for RPs to follow to demonstrate they have addressed the SyAPs. It is the RP's responsibility to determine and describe this detail and for ONR to assess whether the arrangements are adequate.

2.6 This TAG focuses on the assessment of generic security arrangements of the RP's design and does not deal with the administrative security arrangements for handling Sensitive Nuclear Information (SNI) or vetting of individuals. The RP must comply with relevant UK legislation to ensure protection of SNI.

## 3. RELATIONSHIP TO RELEVANT LEGISLATION

3.1 The GDA process sits outside the formal ONR regulatory 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.

## 4. RELATIONSHIP TO IAEA DOCUMENTATION AND GUIDANCE

4.1 The International Atomic Energy Agency (IAEA) document 'Nuclear Security Recommendations on the Physical Protection of Nuclear Material and Nuclear Facilities' Nuclear Security Series (NSS) No 13 (INFCIRC225 Revision 5) (Reference 4) contains principles and recommendations the UK is obligated to take into account.

4.2 The IAEA Technical Guidance documents 16 'Identification of Vital Areas at Nuclear Facilities' (Reference 5) and 4 'Engineering Safety Aspects of the Protection of Nuclear Power Against Sabotage' (Reference 6) provide further guidance.

4.3 This TAG is consistent with the principles described in the international and national documents highlighted below.

4.4 The IAEA document INFCIRC225 Revision 5 at paragraphs 3.45 to 3.47, 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).

4.5 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).

## 5. RELATIONSHIP TO NATIONAL POLICY DOCUMENTS

5.1 The SyAPs provide ONR inspectors with a framework for making consistent regulatory judgements on the effectiveness of a dutyholder's security arrangements. This TAG provides guidance to ONR inspectors when assessing a RP's submission demonstrating the generic design of the security measures on a new nuclear power plant.

5.2 The HMG Security Policy Framework (SPF) (Reference 7) describes the Cabinet Secretary's expectations of how HMG organisations and third parties handling HMG information and other assets will apply protective security to ensure HMG can function

effectively, efficiently and securely. The security outcomes and requirements detailed in the SPF have been incorporated within the SyAPs to ensure dutyholders are presented with a coherent set of expectations for the protection of nuclear premises, Sensitive Nuclear Information (SNI), and the employment of appropriate personnel security controls both on and off nuclear premises.

5.3 The Classification Policy (Reference 8) indicates those categories of SNI which require protection and the level of security classification to be applied.

5.4 The Design Basis Threat is detailed in the extant version of the Nuclear Industries Malicious Capabilities (Planning) Assumptions (NIMCA) document (Reference 9). This document refers to the malicious capabilities associated with theft and sabotage that need to be addressed when the RP carries out Vital Area identification and Vulnerability Assessment activities etc.

## 6. ADVICE TO INSPECTORS

6.1 ONR security inspectors should ensure their activities are integrated with those being undertaken by the ONR safety inspectors to help provide a consistent response to the RP. 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. Similarly, ONR security inspectors should verify any design changes arising for safety and/or environmental reasons have take due account of potential impacts on security.

6.2 The objective for the security assessment of the generic design is for ONR to judge whether the proposed arrangements will be adequate to address relevant threats and are capable of being, and likely to be, successfully integrated into the overall site arrangements. These overall arrangements would form the basis of the dutyholder's approved Site Security Plan (SSP).

6.3 ONR security inspectors are required to make judgements in developing their response to the generic design submission documents. The inspector should ensure that the RP has identified all relevant FSyPs and SyDPs and effective processes are in place to achieve these principles. Engagement with the RP throughout the GDA process is essential to fully understand their proposals and influence the quality and completeness of the final submissions. Where there is an opportunity, ONR security inspectors should determine how and why security measures are applied in those reactors of the same design currently operating/under construction elsewhere. This can be a beneficial starting point in determining the RP's understanding of protective security.

6.4 The security assessment should cover target identification and the design basis threat to determine whether the proposed security arrangements are proportionate and effective in meeting the appropriate SyAPs outcomes. This determination will consider whether the arrangements provide adequate mitigation against the risk of sabotage of nuclear facilities or supporting structures, systems and components (SSCs), and sabotage or theft of nuclear or other radioactive material, or compromise of sensitive nuclear information.

6.5 ONR security inspectors should consider whether the RP's submission demonstrates that the proposed generic security measures will meet the appropriate SyAPs security outcomes. Inspectors should further consider the proposals in the context of their application at a UK site and how the generic proposals might be integrated into overall site arrangements by examining claims, arguments and evidence supporting the RP's assertion that the arrangements meet the outcomes.

6.6 ONR security inspectors should ensure that the GSR submission from the RP clearly defines the scope of the plant covered. Should the technology described in the GSR be subsequently deployed in the UK, the assessment of the complete design at the site, possibly as a multi-unit installation, will be focussed initially, on those areas not assessed as a part of the GDA scope.

6.7 It should be remembered that the assessment report produced by ONR security inspectors will subsequently be used by a project developer to support the justification within the SSP for a specific site security arrangements.

6.8 Where there are deficiencies in the final submissions or aspects that need further definition or modification at the close of the GDA process these should be recorded as residual matters. Where these are substantial in scope, quantity or importance they should be recorded as issues. The methodology to record these is found in the GDA process on HOW2.

## 7. GENERIC SECURITY REPORT

7.1 The GSR generated by the RP has a number of key features as described in Section 8. In essence the GSR must identify the targets requiring protection and the features built into the plant to provide protection to those areas, using the defence in depth principle.

7.2 The detail available at the time the GSR is submitted will be dependent on the maturity of the reactor design. The scope of GDA will be agreed with the RP and those areas to be assessed and sampled clearly defined by ONR. Likewise, there should be clear statements regarding those aspects of security that will be developed subsequent to the GDA process by the prospective licensee.

7.3 The development of the GSR may be an iterative process depending on the RP's experience in applying security arrangements and the GSR may require development through the GDA steps. It is important that the inspector can gauge the level of the RP's understanding and this can be achieved by the submission of a preliminary security report which demonstrates how potential targets have been identified and defence in depth applied. The RP may present an existing security plan of a similar design on another site to help articulate their understanding and provide the inspector with a basis to start engagement and assessment.

## 8. KEY FEATURES OF A GENERIC SECURITY REPORT SUBMISSION

### TARGET IDENTIFICATION

8.1 In order to apply effective security arrangements, it is of fundamental importance that those areas requiring protection are appropriately identified. Target identification should be carried out at an early stage of the GDA process to ensure there is sufficient time to consider the potential to design out vulnerabilities or build in necessary security arrangements to mitigate the threat. Targets will include NM & ORM, nuclear facilities, operational technology and some other specific SSCs.

### CATEGORISATION FOR THEFT AND SABOTAGE

8.2 The RP should have an appropriate process in place to identify theft targets through robust categorisation of its NM and ORM inventory. Guidance on identification of theft targets and categorisation can be found in TAG – Target Identification for Theft CNS-TAST-GD 6.1 http://www.onr.org.uk/operational/tech_asst_guides/cns-tast-gd-6.1.pdf

8.3 The GSR should identify Vital Areas (VAs), in line with the UK definition and using the UK Design Basis Threat – NIMCA (Reference 9). Guidance on the identification of Vital Areas is contained within TAG Target Identification for Sabotage – CNS-TAST-GD-6.2. http://www.onr.org.uk/operational/tech_asst_guides/cns-tast-gd-6.2.pdf

8.4 The categorisation of the nuclear and other radioactive material and facilities for both sabotage and theft is essential as this will determine the security outcomes, as detailed in the SyAPs annexes, which need to be achieved.

**CYBER SECURITY**

8.5 The GSR should provide details of Operational Technology and Information Technology (including software) to include:

- Computer Based Systems Important to Nuclear Safety (CBSIS);
- Computer Based Security Systems (CBSy);
- Nuclear Material Accountancy & Control (NMAC);
- Basic Process Control & Instrumentation Systems (BPC&I);
- Any other digital technology systems as necessary.

8.6 The RP should have an appropriate process in place to identify the different types of technology that deliver functions as part of the nuclear security and safety related equipment and software operating at sites. Guidance on identification of technology and categorisation can be found in TAG – Protection of Nuclear Technology and Operations-TAST-GD 7.3. http://www.onr.org.uk/operational/tech_asst_guides/cns-tast-gd-7.3.pdf

8.7 It is important that OT and IT risks are identified and effectively managed. A fundamental aspect of this is categorisation in line with the tables in the SyAPs annexes. Identification and categorisation of OT and IT should allow the RP to design an effective cyber protection system using a graded approach to achieve the relevant cyber security outcome. Further guidance for inspectors can be found in TAG - Effective Cyber and Information Risk Management – TAST-GD-7.1. http://www.onr.org.uk/operational/tech_asst_guides/cns-tast-gd-7.1.pdf

## 9. PROCESS

9.1 ONR security inspectors should become familiar with the general reactor technology. The RP should provide a comprehensive overview of the security arrangements that are in place at an existing site of the same technology and provide evidence of how targets have been identified and threats mitigated. This information can be used by ONR security inspectors as a basis of understanding to identify similarities with SyAPs and relevant TAGs or any gaps or differences of approach that can be addressed early in the GDA process.

9.2 ONR security inspectors should discuss the submission scope and expectations with the RP and their contractors as necessary, and then request the RP to prepare an outline for the proposed layout and content of the GSR. ONR will then review the submission and advise the RP, following discussion if necessary, on the adequacy of the proposed content and layout of the document.

9.3 The GSR and supplementing documentation should identify the security function (delay, detect, assess etc) to be delivered to meet the relevant SyAPs outcomes. The

claim that an outcome is met should be supported by appropriate arguments and evidence to justify the function will be achieved to a defined posture. Examples of evidence may include the construction of the walls, floors or ceilings of areas containing VAs and operational technology, and security access control arrangements.

9.4 The GSR should include sufficient information on access control arrangements and emergency exits, particularly in areas containing NM, ORM, VAs and operational technology. Thus it should be clear how movement into and out of the security zones/areas is controlled during different plant states (commissioning, normal operations, maintenance and outage). Examples of information can include drawings identifying the location of 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. These could include the codes and standards to which the equipment should be designed, manufactured, constructed installed, commissioned, quality assured, maintained, tested and inspected as evidence to support claims made in achieving functional postures. Emergency egress routes into and out of secure areas should also be detailed in the document.

9.5 A high level concept of operations should be delivered by the RP to identify 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 uninterruptable power supplies (UPS) if necessary, should be set down in the GSR even if plans are at a conceptual level.

9.6 It is anticipated that the GSR will include a number of layout drawings as supporting evidence. The RP should verify that all the latest information has been included in the submission. Inspectors should be mindful that the RP's change control process will be vital in ensuring the most up-to-date designs are being assessed.

9.7 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 GSR iterations will be received. The RP should maintain an audit trail that evidences ONR's position and the findings throughout the GDA process. ONR security inspectors should have similar controls in place.

9.8 The verification of the RP-designated VAs and operational technology may be undertaken by assessment by nuclear safety inspectors as part of the GDA process.

## 10. FINAL GSR SUBMISSION

10.1 The final iteration of the GSR forms part of the RP's GDA submission. It will be assessed by ONR Security Inspectors, taking account of all relevant FSyPs and SyDPs and related TAGs. This will assist with compilation of the technical assessment report at the end of the GDA process. Inspectors should verify that the relevant outcomes have been identified and that adequate arguments and evidence to support the achievement of those outcomes have been provided by the RP. The overall decision on the acceptability of the submission should be based on the arguments and evidence within the GSR.

## 11. REPORTING ASSESSMENT FINDINGS

11.1 A reporting format for the GDA assessment reports will be provided to ONR security inspectors 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 a report that does not contain SNI but ensure it gives as much detail as reasonable. ONR security inspectors should consider annexing SNI or producing a

report at a higher classification where it is considered beneficial to expand on the reasons for judgements being made and the content would warrant the higher classification. The report should also describe, openly and transparently, the process followed, the work undertaken and the findings made. The SNI annex or separate report should not be published on the ONR website, but should be shared with RPs.

## 12. REFERENCES

1. ONR Security Assessment Principles

2. Nuclear Industries Security Regulations (NISR) 2003 (as amended) Statutory Instrument 2003 no.403

3. ONR Generic Design Assessment Guidance to Requesting Parties

4. IAEA Nuclear Security Series No.13 – Nuclear Security Recommendations on the Physical protection of Nuclear material and Nuclear facilities (INFCIRC/225/Revision 5) January 2011. www-pub.iaea.org/MTCD/Publications/PDF/Pub1481_web.pdf

5. IAEA Nuclear Security Technical Guidance Document No.16 – Identification of Vital Areas at Nuclear Facilities http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1505_web.pdf

6. IAEA Technical Guidance Document Engineering Safety Aspects of the Protection of Nuclear Power Against Sabotage www-pub.iaea.org/MTCD/Publications/PDF/Pub1271_web.pdf

7. HMG Security Policy Framework

8. NISR Classification Policy for the Civil Nuclear Industry

9. Nuclear Industries Malicious Capabilities (Planning) Assumptions

## 13. GLOSSARY AND ABBREVIATIONS

| | |
|---|---|
| BPC&I | Basic Process Control & Instrumentation |
| CBSIS | Computer Based Systems Important to Safety |
| CBSy | Computer Based Security Systems |
| CNS | Civil Nuclear Security |
| GDA | Generic Design Assessment |
| GSR | Generic Security Report |
| IAEA | International Atomic Energy Agency |
| IT | Information Technology |
| NIMCA | Nuclear Industries Malicious Capabilities (Planning) Assumptions |
| NISR | Nuclear Industries Security Regulations |
| NM | Nuclear Material |
| NMAC | Nuclear Material Accountancy & Control |
| NSSP | Nuclear Site Security Plan |
| ONR | Office for Nuclear Regulation |
| ORM | Other Radioactive Material |
| OT | Operational Technology |
| RP | Requesting Party |
| SNI | Sensitive Nuclear Information |
| SPF | Security Policy Framework |
| SSCs | Structures, Systems, Components |
| SSP | Site Security Plan |
| SyAPs | Security Assessment Principles |
| TAG | Technical Assessment Guide |
| UPS | Uninterruptable Power Supply |
| VA | Vital Area |
| VAI | Vital Area Identification |