ONR GUIDE			
RELIABILITY AND RESILIENCE OF THE SECURITY SYSTEM			
Document Type:	Nuclear Security Technical Assessment Guide		
Unique Document ID and Revision No:	CNS-TAST-GD-5.1 Revision 1		
Date Issued:	March 2020	**Review Date:**	March 2023
Approved by:	Matt Sims	Professional Lead	
Record Reference:	TRIM Folder 4.4.2.19075. (2019/135638)		
Revision commentary:	Fit for Purpose Review of Revision 0		

TABLE OF CONTENTS

Published 03/20

1. INTRODUCTION

1.1 The Office for Nuclear Regulation (ONR) has established a set of Security Assessment Principles (SyAPs) (Reference 7). 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 (NISR) 2003 (Reference 1).

1.2 The term 'security plan' is used to cover all dutyholder submissions such as nuclear site security plans, temporary security plans and transport security statements. NISR Regulation 22 dutyholders may also use the SyAPs as the basis for Cyber Security and Information Assurance documentation that helps them demonstrate ongoing legal compliance for the protection of Sensitive Nuclear Information (SNI). 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.

2. PURPOSE AND SCOPE

2.1 This TAG contains guidance to advise and inform ONR inspectors in exercising their regulatory judgment during assessment activities relating to a dutyholder's arrangements to ensure their security systems have appropriate levels of reliability and resilience. 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 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.

3. RELATIONSHIP TO LEGISLATION

3.1 The term 'dutyholder' mentioned throughout this guide is used to define 'responsible persons' on civil nuclear licensed sites and other nuclear premises subject to security regulation, a 'developer' carrying out work on a nuclear construction site and approved carriers, as defined in NISR. It is also used to refer to those holding SNI.

3.2 NISR defines a 'nuclear premises' and requires 'the responsible person' as defined to have an approved security plan in accordance with Regulation 4. It further defines approved carriers and requires them to have an approved Transport Security Statement in accordance with Regulation 16. Persons to whom Regulation 22 applies are required to protect SNI. ONR considers reliability, resilience and sustainability to be important components of a dutyholder's arrangements in demonstrating compliance with relevant legislation.

4. RELATIONSHIP TO IAEA DOCUMENTATION AND GUIDANCE

4.1 The essential elements of a national nuclear security regime are set out in the Convention on the Physical Protection of Nuclear Material (CPPNM) (Reference 4) and the IAEA Nuclear Security Fundamentals (Reference 3). Further guidance is available within IAEA Technical Guidance and Implementing Guides.

4.2 Fundamental Principle J of the CPPNM refers to quality assurance and states that a quality assurance policy and quality assurance programmes should be established and

implemented with a view to providing confidence that specified requirements for all activities important to physical protection are satisfied. The importance of issues relating to quality assurance is also recognised in the Nuclear Security Fundamentals, specifically:

- Essential Element 12: Sustaining a Nuclear Security Regime – 3.12 A nuclear security regime ensures that each competent authority and authorised person and other organisations with nuclear security responsibilities contribute to the sustainability of the regime by:
    - Allocating sufficient human, financial and technical resources to carry out the organisation's nuclear security responsibilities on a continuing basis using a risk-informed approach
    - Routinely conducting maintenance, training and evaluation to ensure the effectiveness of the nuclear security systems
    - Routinely performing assurance activities to identify and address issues and factors that may affect the capacity to provide adequate nuclear security, including cyber security, at all times

4.3 A more detailed description of the quality assurance is provided in Recommendations level guidance, specifically Nuclear Security Series (NSS) 13, Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5) (Reference 2). This document states "The quality assurance policy and programme(s) for physical protection should ensure that a *physical protection system* is designed, implemented, operated and maintained in a condition capable of effectively responding to the *threat assessment* or *design basis threat* and that it meets the State's regulations, including its prescriptive and/or performance based requirements."

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 dutyholder's submission demonstrating they have effective processes in place to achieve SyDP 5.1 – Reliability and Resilience, in support of FSyP 5 – Reliability, Resilience and Sustainability. The TAG is consistent with other TAGs and associated guidance and policy documentation.

5.2 The HMG Security Policy Framework (SPF) (Reference 5) 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. This ensures that dutyholders are presented with a coherent set of expectations for the protection of nuclear premises, SNI and the employment of appropriate personnel security controls both on and off nuclear premises.

5.3 The Classification Policy (Reference 6) indicates those categories of SNI, which require protection and the level of security classification to be applied.

6. ADVICE TO INSPECTORS

6.1 It is particularly important to ensure, so far as possible, that the security system is capable of performing its function with an adequate level of reliability. This objective may be achieved by the adoption of a number of different provisions, together with the use of techniques to demonstrate the adequacy of the specified measures. The reliability of plant and systems to provide the security effect should be demonstrated by the dutyholder to be consistent with the risks associated with the loss of this capability. This should be informed by the Category of the security function and the Classification of the security structure, system or component (SySSC) concerned.

6.2 The security system design should incorporate an appropriate level of redundancy to reduce the effects of random failure, and diversity and segregation to reduce the effects of common cause failure and malicious actions. This should take account of the site or facility the system is protecting and its vulnerability to threats described in the Design Basis Threat (DBT) (Reference 8).

6.3 In assessing the fitness for purpose of the security system, and particularly the ability to deliver a particular effect, a number of issues relating to redundancy and diverse provisions should be considered. Security plans should clearly identify the security function of all SySSCs so that this assessment can be carried out.

Regulatory Expectation

6.4 There is a regulatory expectation that dutyholders demonstrate in the security plan how they ensure that the design and operation of the security system delivers appropriate levels of redundancy, diversity and segregation. Dutyholders should provide sufficient resources (including personnel) to inform the design, to maintain and to restore SySSCs, thus building resilience to enable an appropriate and effective incident response, and a recovery programme that reflects the risk of any loss of service. Essential services critical to the correct functioning of the security system should be given the same priority as the system itself and as such are required to have appropriate levels of reliability and resilience.

FSYP 4 - Reliability, Resilience and Sustainability	Reliability and Resilience	SyDP 5.1
Security structures, systems and components should be appropriately qualified, with design incorporating reliability and resilience through ‘failsecure’, redundancy, diversity and segregation. There should also be sufficient resources available and contingency arrangements developed to ensure continuity of security provision.		

7. ELEMENTS OF SYSTEM RESILIENCE

Redundancy

7.1 Redundancy is frequently defined as the provision of more than the minimum number of equipment items, components or elements required to perform a specific security function. Such redundancy allows a specified security function to be delivered when one or more items (but not all) are unavailable, due to a variety of unspecified potential failure mechanisms or maintenance (e.g. identified faults or hazards).

7.2 Experience dictates there are deterministic and probabilistic arguments to justify the provision of redundancy in SySSCs. A design which is considered acceptable will display adequate levels of system redundancy to ensure it is fit for purpose and should perform the required security function. These characteristics will include final provisions to satisfy the deterministic and probabilistic requirements of any potential design for SySSCs.

Dependent Failure

7.3 A possible threat to SySSC resilience is that posed by dependent failure. These have the potential to prevent the performance of a required security function through simultaneous loss of redundancy provisions. Particular illustrations of this type of failure are common-cause failures (CCF).The inspector should be satisfied that the risk from dependent failures has been reduced to a level which is acceptable within the limits set by design requirements. It is important to note that reliability does not necessarily increase indefinitely in proportion to levels of redundancy, and this is primarily due to common origin or common cause effects. This type of failure is often referred to either as CCF or a common mode failure (CMF). A CCF is a dependent failure event where approximately simultaneous multiple failures result from a single shared cause (e.g. fire). A CMF is a common cause event where multiple equipment items fail in the same mode.

7.4 Multiple failures can occur due to common weaknesses or dependencies shared by components. Such failures can cause failure of all redundant components in a single security system or failure of components in more than one system. Dependent failures can considerably reduce the reliability of the security systems relative to that expected of random failures occurring in isolation.

7.5 The main types of dependencies which could cause potential loss of a security function are described below.

- **Functional dependencies**, which arise from shared or common functional features; such as a common electrical power source, common wiring or a shared communication node.
- **Spatial dependencies**, which arise from physical features shared by components located in a common location; such as common radiation or chemical conditions, a common environment and support structures, and vulnerability to leaks of dangerous fluids (high temperature, corrosive or toxic) or anything else potentially attributable to SySSCs' common location.
- **Inherent dependencies**, which arise from shared characteristics; such as a common principle of operation or technical feature such as electrical overload.
- **Human error related dependencies**, which arise from human errors affecting some shared or common human process; such as human error in design or manufacture, or staff error during operation and maintenance.

7.6 To provide protection against dependent failures, the inspector should seek confirmation that the dutyholder has identified and, where necessary and practicable, implemented measures in design, construction and operation to eliminate them or reduce their potential effect. Examples of such measures are:

- the provision of segregation to eliminate spatial dependencies;
- the avoidance of functional dependencies by segregation of SySSCs and their support services;
- the provision of alternative and independent equipment to eliminate undue reliance on any single system. The purpose of this approach is to help provide protection against any 'hidden failure dependencies' that may not be identified; and
- approaches and procedures should be implemented to minimise the possibility of failure dependencies arising during design, manufacture, construction and operation, including dependencies due to operator and other human error.

Diversity

7.7 Where a component of the security system is at potential risk from common cause failures, one means of reducing the susceptibility is to employ diverse provisions in separate redundant trains or systems. For example, the detect function over a given area could be delivered by both fixed-line and pan-tilt-zoom closed circuit television powered by segregated electricity supplies and supported by a dual perimeter intruder detection system utilising complementary technologies (for example infrared and microphonic technologies), again powered by segregated power supplies. A dutyholder should consider appropriate measures to include diversity within the components of the system which is designed to deliver an individual effect and/or across SySSCs in their entirety. Engineering diversity is defined as the provision of dissimilar means of achieving the same objective; e.g. the use of features which differ in the physical means of achieving a specific objective or use of different equipment made by different manufacturers.

7.8 Diversity provides one means of protection against some causes of failure, by removing common features which may lead to failure dependencies. Diversity particularly provides protection against inherent dependencies and human error related dependencies.

7.9 The physical co-location or functional support of diverse systems could lead to dependencies that defeat the objective of providing diversity. This should be addressed through the layout and functional design of the SySSC where appropriate.

Segregation

7.10 In a resilient SySSC, despite diverse provisions, the threat of common cause failures from hazards such as fire or hostile intent may be reduced by system segregation. This is the separation of components by distance or physical barriers, a particular example being provision of principal fire barriers to delineate individual fire zones; they may also serve as barriers to other hazards such as blast. Appropriate levels of segregation should be present in a dutyholder’s provisions in order to maximise the likelihood that a security function will be performed, despite the occurrence of faults and hazards, possibly in combination.

7.11 Equipment segregation is the separation of redundant and/or diverse components by distance or by barriers in order to prevent all (or sufficient to enable system failure) of the components being damaged, particularly in the event of common hazards or

malicious action. A system's design should ensure that internal hazards, such as fire and certain external threats do not damage separate chains of security equipment to the extent that its functional reliability is unacceptably reduced. The most straightforward manner in which segregation can be achieved is through distance and avoiding collocating components.

System Independence

7.12 SySSC may be subject to spurious operation in addition to operational failures. These can arise because a given system component does not possess a sufficient level of independence from other separate systems. Measures need to be employed by the dutyholder to ensure that, wherever possible, SySSCs are not adversely affected by the spurious operation or failure of other systems, especially through any potential for hidden dependency (for example, by having a single system responsible for fire and security response). This is best achieved by designing in both functional and physical isolation.

8. SUITABLY QUALIFIED AND EXPERIENCED PERSONNEL

8.1 The dutyholder's security organisation should possess adequate Suitably Qualified and Experienced (SQEP) personnel to support SySSCs. This includes having sufficient personnel with the necessary competences and knowledge to manage, operate, maintain and repair security systems at all times.

9. ESSENTIAL SERVICES AND THE SECURITY SYSTEM

Where essential services (such as computer based security systems) are necessary to support the functioning of a Physical Protection System (PPS), then these services should be sufficiently resilient and secure to ensure that their loss or interruption does not adversely affect the ability of the PPS to achieve the required outcome as defined in SyAPs Annexes C and D.

Inspectors should consider:

- Has reliability, resilience and sustainability been considered throughout the design stage for any new facility or SySSC and incorporated within relevant operational requirements or equivalent?
- Are requirements for SySSCs regularly reassessed in conjunction with all stakeholders?
- Are there sufficient SQEP and other resources to manage, operate, maintain and repair the SySSC?
- Does the design and operation of the SySSC display appropriate levels of redundancy, diversity and segregation?
- Do essential services (such as power) necessary for the correct functioning of the SySSC have the appropriate levels of security, reliability and resilience?
- Have potential dependencies and/or vulnerabilities of the SySSC been identified and mitigated?

- Do SySSCs ‘fail secure’ and, if they do not, are security requirements appropriately balanced against safety requirements and are adequate compensatory security measures available?
- Does the dutyholder demonstrate the ability to learn from their experience in maintaining a SySSC?
- Is there a process of continuous improvement in place in relation to SySSCs’ reliability, resilience and sustainability?
- Are appropriate quality performance and assurance mechanisms applied to SySSC?
- Is the response to the failure or loss of part of or all of a SySSC regularly exercised or rehearsed?

10. REFERENCES

1. **Nuclear Industries Security Regulations 2003**. Statutory Instrument 2003 No. 403

2. **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.

3. **IAEA Nuclear Security Series No. 20**. Objective and Essential Elements of a State's Nuclear Security Regime. http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1590_web.pdf

4. **Convention on the Physical Protection of Nuclear Material (CPPNM)** https://ola.iaea.org/ola/treaties/documents/FullText.pdf

5. **HMG Security Policy Framework**. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/710816/HMG-Security-Policy-Framework-v1.1.doc.pdf

6. **NISR 2003 Classification Policy** http://www.onr.org.uk/documents/classification-policy.pdf

7. **Security Assessment Principles** – Trim Ref. 2017/121036

8. **Design Basis Threat**

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

11. GLOSSARY AND ABBREVIATIONS

BC	Business Continuity
CCF	Common Cause Failure
CMF	Common Mode Failure
CPNI	Centre for the Protection of National Infrastructure
CPPNM	Convention on the Physical Protection of Nuclear Material
DBT	Design Basis Threat
FSyP	Fundamental Security Principle
IAEA	International Atomic Energy Agency
NIMCA	Nuclear Industries Malicious Capabilities Planning Assumptions
NISR	Nuclear Industries Security Regulations
NSS	Nuclear Security Series
ONR	Office for Nuclear Regulation
PPS	Physical Protection System
SNI	Sensitive Nuclear Information
SPF	Security Policy Framework
SQEP	Suitably Qualified and Experienced
SySSC	Security Structure, System and Component
SyAP	Security Assessment Principle
SyDP	Security Delivery Principle
TAG	Technical Assessment Guide