Identification and Analysis of Security Tasks and Roles			
Doc. Type	ONR Technical Assessment Guide (TAG)		
Unique Doc. ID:	CNS-TAST-GD-3.1	**Issue No.:**	3.1
Record Reference:	2022/14756		
Date Issued:	Apr-22	**Next Major Review Date:**	Apr-27
Prepared by:		Principal Inspector	
Approved by:		Superintending Inspector	
Professional Lead:		Superintending Inspector	
Revision Commentary:	Minor typographical updates to Issue 3.		

Table of Contents

1. Introduction

1. ONR has established its assessment principles, which apply to the assessment by ONR specialist inspectors of safety, security and safeguards submissions for nuclear facilities or transports that may be operated by potential licensees, existing licensees, or other dutyholders.
These assessment principles are supported by a suite of guides to further assist ONR's inspectors in their technical assessment work in support of making regulatory judgements and decisions against all legal provisions applicable for assessment activities. This technical assessment guide (TAG) is one of these guides.

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. Dutyholders under Regulation 22 of the Nuclear Industries Security Regulations 2003 ('NISR') [1] may also use ONRs Security Assessment Principles (SyAPs) [2] as the basis for Cyber Security and Information Assurance (CS&IA) 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 TAG is such a guide.

2. Purpose and Scope

3. This TAG contains guidance to advise and inform ONR inspectors in exercising their regulatory judgment during assessment activities relating to a dutyholder's identification, analysis and substantiation of security tasks and roles. 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.

3. Relationship to Relevant UK Legislation and Policy

4. 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.

5. NISR defines a ‘nuclear premises’ and requires ‘the responsible person’ as defined to have an approved security plan in accordance with Regulation 4. This regulation includes a requirement to ensure the security of equipment and software used in connection with activities involving Nuclear Material (NM) or Other Radioactive Material (ORM). NISR 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 CS&IA to be an important component of a dutyholder’s arrangements in demonstrating compliance with relevant legislation.

6. The SyAPs provide ONR inspectors with a framework for making consistent regulatory judgements on the effectiveness of a dutyholder’s security arrangements. This TAG is part of a suite supporting FSyP 3 – Management of Human Performance - and provides guidance to ONR inspectors when assessing a dutyholder’s submission demonstrating they have effective processes in place to achieve SyDP 3.1 – Identification and Analysis of Security Tasks and Roles. The TAG is consistent with other TAGs and associated guidance and policy documentation.

7. The Government Functional Standard on security [3] describes expectations for security risk management, planning and response activities for cyber, physical, personnel, technical and incident management. It applies, whether these activities are carried out by, or impact, the operation of government departments, their arm’s length bodies or their contracted third parties. The security principles, governance, life cycle and practices detailed within Functional Standard have been incorporated within SyAPs. This ensures that all NISR dutyholders are presented with a coherent and consistent set of regulatory expectations for protective security whether they are related to government or not.

8. The Government Security Classifications document, together with ONR’s Classification Policy [4] describe types of information that contain SNI, the level of security classification that should be applied, and the protective measures that should be implemented throughout its control and carriage.

4. Relationship to International Standards and Guidance

9. The essential elements of a national nuclear security regime are set out in the Convention on the Physical Protection of Nuclear Material (CPPNM) [5] and the IAEA Nuclear Security Fundamentals [6]. Further guidance is available within IAEA Technical Guidance and Implementing Guides.

10. Fundamental Principle E of the CPPNM refers to the responsibility of dutyholders to implement a Physical Protection System (PPS). It details that the State should ensure that the prime responsibility for the implementation of physical protection of nuclear material or of nuclear facilities rests with the holders of the relevant licenses or of other authorising documents.
The importance of physical protection of Nuclear Material (NM) and Other Radioactive Material (ORM) is also recognised in the Nuclear Security Fundamentals, specifically Essential Element 3: Legislative and Regulatory Framework – 3.3 The legislative and regulatory framework, and associated administrative measures, to govern the nuclear security regime should provide for the establishment of systems and measures to ensure that NM and ORM are appropriately accounted for or registered and are effectively controlled and protected.

11. Fundamental Principle I of the CPPNM refers to the concept of several layers and methods of protection (structural or other technical, personnel and organisational) afforded by the PPS. A more detailed description of the graded approach is provided in Recommendation's level guidance, specifically Nuclear Security Series (NSS) 13 [7]. This document states that dutyholders should prepare a security plan based on a threat assessment or the design basis threat and should include sections dealing with design, evaluation, implementation, and maintenance of the PPS. Sections 4, 5 and 6 contain more detailed guidance on specific measures that dutyholders should adopt to protect NM/ORM against theft and sabotage.

12. The importance of issues relating to human performance are also recognised in the Nuclear Security Fundamentals, specifically:

- Essential Element 12: Sustaining a Nuclear Security Regime – 3.12:
    - d) 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; and
    - e) Routinely conducting maintenance, training, and evaluation to ensure the effectiveness of the nuclear security systems.

13. A more detailed description of the elements is provided in NSS 13 [7].
This publication highlights the importance of designing robust Physical Protection Systems including engineered and operational security measures,

evaluating and demonstrating their effectiveness. It also highlights the importance of ensuring integrated solutions that manage the interface with safety systems to avoid adverse impact and to ensure they are mutually supportive.

5. Advice to Inspectors

14. Humans play a key role in the delivery of nuclear security, forming an integral part of the protective security arrangements and response to a nuclear security event. Effective human performance is fundamentally dependent on assuring that the assignment of tasks in a system best matches the capabilities of its human and engineered components. Where tasks are assigned to humans these must be designed to optimise human performance whist minimising the likelihood of human failure.

15. It is essential that all personnel whose activities have the potential to impact on nuclear security can deliver their role reliably. Therefore, robust arrangements for identifying reliance upon humans to deliver nuclear security and assuring that these tasks are suitably supported is essential for an organisation to achieve secure operations.

16. Effective arrangements for the management of human performance typically include identifying and analysing security tasks and roles, and then ensuring that these tasks are designed to match the information processing and physical capabilities of humans. This is achieved through:

    - Ensuring adequate numbers of demonstrably competent staff are available and fit for duty (SyDP 3.2);
    - Providing staff with suitable workspaces, equipment and interfaces which are designed to meet the demands of their tasks (SyDP 3.3);
    - Ensuring personnel are guided by well-designed administrative controls including normal and emergency security operating procedures (SyDP 3.4).

17. This TAG informs regulatory assessment of FSyP 3 Management of Human Performance and specifically addresses aspects of identification and analysis of tasks important to the creation of an effective nuclear security regime that will consistently deliver the expected Security Outcomes (see SyAPs Annexes and CNS-TAST-GD-6.3 [8] for further detail on Security Outcomes). In order to ensure that tasks are designed to match human capabilities, it is necessary that the task demands are understood and that the potential for failure (system fault or human error) that would prevent Security Functions[1] being achieved is identified. Identification of tasks important to nuclear security is a key initial step in this process. The analysis and understanding of tasks are then used to inform: the staffing design and competence management arrangements, the task environment, and the design of equipment and procedures. All of which is required to support achievement of reliable human performance to an

[1] A Security Function is a specific purpose or objective that must be accomplished so that the overall nuclear security Outcome can be achieved.

established standard and to deliver the required Security Outcomes. This TAG establishes ONR's expectations of the dutyholder's arrangements for:

- Identification of nuclear security tasks.
- Assigning a proportionate analysis of these tasks, focusing on those important to the delivery of nuclear security functions.
- Substantiation of the suitability of the design of the security measure including the (Security Structure, System or Component) SySCC and actions required for operation and maintenance of the SySCC to reliably deliver the relevant security function.

18. This guidance should be applied in a proportionate and targeted manner during assessment of security plans for all stages of operations. This includes security plans that cover the design and modification of new and existing facilities and justification of the adequacy of existing operations and decommissioning. In addition, such analysis should be applied where shortfalls in engineered controls are compensated for by administrative controls either on a temporary or permanent basis.

19. This assessment guide focuses on the identification and analysis of nuclear security tasks and roles. It highlights the importance that ONR places on the adoption of a systematic approach to the identification and analysis of tasks and provides high level guidance for inspectors on some of the formal methods that can be applied for this purpose.

6. Regulatory Expectation

20. The regulatory expectation placed upon the dutyholder is that they will ensure that the security plan identifies how they identify and analyse tasks important to nuclear security to demonstrate that they are designed so that they can be undertaken effectively minimising the likelihood of human failure.

FSyP 3 – Management of Human Performance	Identification and Analysis of Security Tasks and Roles	SyDP 3.1
A systematic approach to the identification and analysis of all tasks important to security should be undertaken, which demonstrates that tasks assigned to those with security roles are designed so that they can be effectively delivered.		

7. Systematic Approach for the Identification of Tasks Important to Nuclear Security

21. Having a systematic process in place by which Tasks Important to Nuclear Security (TINS) are identified and allocated to personnel is a key component of human performance management. TINS may be distributed amongst persons with identified security roles as well as other personnel such as directors, designers, managers, operators and maintainers, and those involved in the conduct of security risk assessments and the production of security plans.

22. The identification of tasks should encompass:

- tasks required for the protection of Nuclear Material, Other Radioactive Material and associated facilities against acts of theft and sabotage;
- security tasks involved with the transport of nuclear and radioactive material by Class A and B carriers;
- tasks required to protect confidentiality, integrity and availability of SNI;
- security tasks required to support nuclear safety events.

23. The identification of TINS should consider tasks completed by direct employees as well as contracted elements of the workforce whose activities may impact upon nuclear security.

24. The identification of TINS should include all the tasks that are required to achieve Security Functions. These may take the form of procedural or administrative controls that form part of the protective security arrangements. Procedural and administrative controls are considered to be human based controls, i.e., controls where the security function is delivered primarily by a human task e.g., a guard force pass check to prevent unauthorised access. Other controls may be wholly engineered or hybrid, where an engineered control requires some human tasks, such as initiating the control for the security function to be delivered e.g., closing electronic outer hostile vehicle mitigation gates. Tasks important to security will also include those tasks that are completed in support of passive and active engineered security controls that form part of the protective security arrangements, i.e., Examination, Inspection, Maintenance and Test (EIMT) tasks.

25. When identifying TINS dutyholders should ensure that all tasks which provide procedural or administrative security measures to deliver the security functions of the PPS are included as well as tasks required in support of engineered

controls. This should include tasks required to deliver or support Security Functions that:

- **Delay** a security threat or attack with sufficient delay in order to achieve the required outcome
- **Detect** a security threat or attack.
- **Assess** the nature of any event and determine the appropriate response.
- Prevent **Unauthorised Access Control** to the site and specific areas within the site.
- Use **Insider Threat Measures** to mitigate insider threats.

26. Similarly, when considering security functions provided by the Cyber Protection System (CPS), the dutyholder's security plan should identify those TINS that deliver or support the Security Functions of:

- **Identify** - Asset Management, Business Environment, Governance, Risk Assessment, Risk Management Strategy
- **Defend** - Access Control, Awareness and Training, Data Security, Information Protection Processes and Procedures, Maintenance, Protective Technology
- **Detect** - Anomalies and Events, Security Continuous Monitoring, Detection Processes
- **Respond** - Response Planning, Communications, Analysis, Mitigation, Improvements
- **Recover** - Recovery Planning, Improvements, Communications

27. The tasks which provide or contribute to the delivery of nuclear security functions, will ultimately need to be substantiated in a proportionate manner as part of the vulnerability analysis that forms part of the Dutyholder's security plan. It is important therefore that they are included in the identification of TINS and are explicitly linked to the security functions they deliver.

28. In addition, tasks which contribute to the overall achievement of security performance should be identified. These additional tasks may include tasks completed by staff who form part of the security team, e.g., security risk analysts and security plan authors, whilst others may be undertaken by staff for whom security responsibilities are only a part of their role, e.g., directors, managers, internal assurance, emergency controllers and operating staff whose primary role will interface and interact with the security system. It is important that these additional security tasks are identified so that training and competence requirements, and procedural requirements associated with the

tasks can be identified and delivered effectively. Whilst these tasks may not need to be formally substantiated, inspectors may direct attention to them when conducting assessments focussed on matters covered by other SyDPs related to FSyP3.

29. Inspectors should consider:

- Has the dutyholder employed a systematic approach to the identification of tasks important to nuclear security and are these clearly documented in the security plan or supporting documents?
- Does the dutyholder's identification of tasks important to nuclear security encompass the full range of activities including transport of nuclear and radioactive materials on or between sites?
- Does the dutyholder's identification of tasks include all procedural and administrative controls that comprise the PPS, CPS and Information Assurance arrangements?
- Does the dutyholder's identification of tasks important to nuclear security include tasks required to support engineered and technological controls in the PPS, CPS and Information assurance arrangements?
- Has the dutyholder identified the totality of tasks to be undertaken by those who have a direct role in the delivery of security?
- Does the dutyholder's approach for the identification of tasks important to security include tasks completed by staff who do not provide security-specific roles?
- Does the dutyholder's process for the identification of tasks important to security encompass roles provided by contract or agency staff as well as direct employees?

8. Assigning a Proportionate Analysis of Tasks Important to Nuclear Security

30. It is important to identify TINS in order to ensure that the demands they place on personnel are understood and that the tasks themselves can be designed to match human capabilities and limitations, increasing the reliability of task performance. Inspectors should recognise that some tasks will have a more important role than others for the maintenance and delivery of nuclear security and therefore it should be expected that a proportionate approach to the analysis of security tasks should be taken by dutyholders.

31. Inspectors should consider the adequacy of the approach dutyholders take to the analysis of TINS. It should be expected that dutyholders are able to articulate a graded approach to both the analysis and substantiation of security important tasks. Several approaches to the selection of tasks for analysis and the depth of analysis applied to substantiate tasks could be applied. ONR does not prescribe the basis on which dutyholders should determine the amount and type of evidence that is required to substantiate tasks important to nuclear security. A number of the Key Security Plan Principles (KSyPP) e.g., those related to the Graded Approach (KSyPP 3), Defence in Depth KSyPP 4), Security Functional Categorisation and Classification (KSyPP 5) and Codes and Standards (KSyPP 7) can provide a sound basis for dutyholders in determining their approach to proportionate analysis and substantiation of security important tasks.

32. Through the security risk assessment process, the importance of the security functions to be delivered should be clearly understood based on the PPS/CPS outcome that needs to be achieved. KSyPP 5 provides one means by which the importance of a Security Function can signified by the assignment of a security function category.

33. Security Functions are delivered by the provision of Security Measures. Security Measures can comprise one or more Security Structures, Systems and Components (SySSC) and TINS (this is illustrated in Figure 1). KSyPP5 also provides a means by which the importance of security measures and their constituent parts can be signified. This is a process known as classification. Detailed advice on the categorisation of nuclear security functions and classification of Security Measures SySSCs is provided in CNS-TAST-GD-11.4.5 [9].

34. The approach to security functional categorisation and classification described by KSyPP5 mirrors that in place for safety functional categorisation and classification and should be familiar to those with a nuclear risk assessment background. TINS should be classified in a similar manner to SySCCs [9].

35. Whilst the KSyPPs describe a formal categorisation and classification process that can be used to signify the importance of a TINS, it is not essential that

dutyholders adopt such an approach. They should however be able to demonstrate an approach that is structured and systematic and which articulates the relative importance of the security measures including all of the TINS that make up their PPS and CPS. This should take into account the contribution the security measure makes to the achievement of the security outcome, its position in the hierarchy of controls and the role it provides in delivering defence in depth.

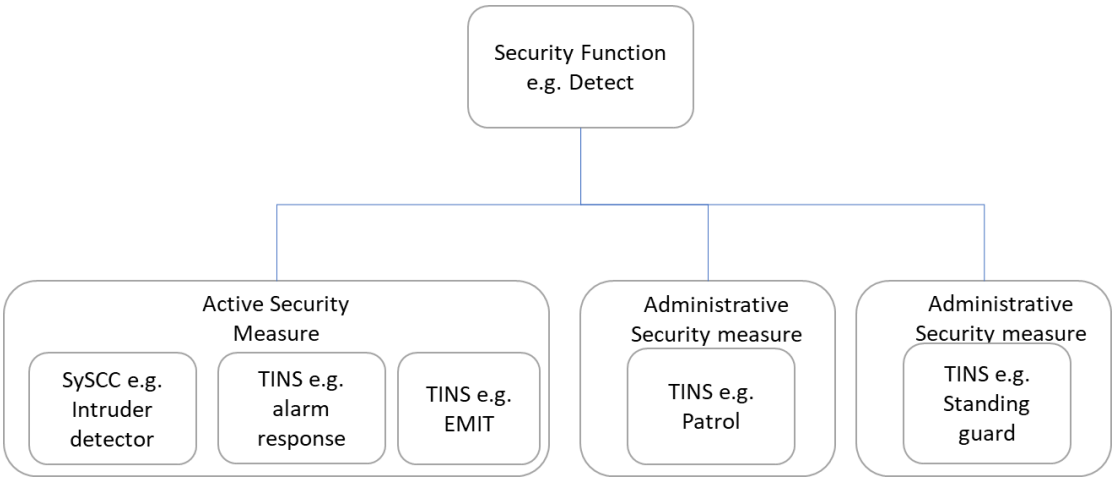

Figure 1: Relationship of Security Functions, Security Measures, SySCCs and TINS

36. The importance (class) of a task should be the main factor that determines the depth of analysis and level of evidence required to substantiate it can reliably deliver a security function. Additional factors that dutyholders might use to determine this include features of the task such as its difficulty or frequency of delivery. Where dutyholders are assigning difficult or infrequent tasks to personnel, these may require more detailed assessment and evidence to substantiate their ability to deliver security functions, than tasks that are simple and commonly assigned to the human part of the arrangements.

37. Inspectors should consider:

- Does the dutyholder have a structured, systematic and proportionate approach for the identification and substantiation of Tasks Important for Nuclear Security?
- Are the results from this approach documented so that the output from it is transparent, consistent and auditable?
- Does the dutyholder's approach and decision-making process include consideration of appropriate factors i.e., security outcome, and security function to be achieved, the importance of the role of the human based security task in achieving the security function and the associated complexity and novelty of the human task(s)?

9. Substantiation of Tasks Important to Nuclear Security

38. Analysis of tasks that provide or support delivery of security functions can take a number of forms and will result in the production of different forms of substantiation evidence. ONR does not endorse any specific method but considers a graded approach could be achieved using three approaches to the analysis and production of evidence to substantiate claims made on human performance for the delivery of nuclear security functions. These require progressively more detailed assessment to be conducted and evidence to be provided as the importance of a human task increases (for example from class 3 to class 1).

39. At the simplest level (level 1), substantiation evidence can be provided by a dutyholder demonstrating that their design of TINS adopts a process in which the design of tasks takes account of human capabilities and limitations, and then applies human factors relevant good practice to their design in order to ensure delivery of security functions. Evidence of this can be provided by recourse to the dutyholder's arrangements and evidence of the application and compliance with standards during design or through specification of Commercial Off the Shelf (COTS) equipment.

40. The next level of analysis (level 2) should, in addition to the integration of human factors during design, provide evidence that TINS deliver the security functions and required outcome determined by the nuclear security risk analysis. This evidence may be provided on the basis of trials of tasks as they are developed, including Factory Acceptance Testing (FAT), from the results of formal exercises of the security system or from operational experience data. Where evidence to substantiate the effectiveness of tasks is based on data of this type inspectors should ensure that the trials test task performance in a realistic manner, e.g., across a range of conditions and demonstrate adequate performance under the most onerous conditions. In addition to the collection of data, dutyholders should demonstrate that review and analysis of this data is undertaken and that improvements to the task are made where evidence of inadequate performance is found.

41. Evidence that demonstrates a high degree of confidence that security functions will be delivered (level 3), in addition to evidence at levels one and two, comes from the application of formal human factors methods to provide a qualitative human reliability analysis. Evidence of this type is likely to require input from human factors professionals and should demonstrate that the tasks required to deliver and support the security measure are fully understood, match human capabilities, are designed so the likelihood of human failure is minimised and that the design of performance influencing factors (staffing and competence arrangements, procedures, equipment and user interfaces) are suitable to support the required levels of task reliability.

42. Qualitative human reliability analysis for the substantiation of TINS at level 3 comprises four main components:

- Task Analysis.
- Allocation of Function
- Human Failure Analysis.
- Assessment of Performance Influencing Factors.

43. Each of these components can be conducted using a range of methods and guidance is provided on each of these in Appendix 2. ONR does not endorse any specific method to be applied, however, inspectors should ensure that dutyholders justify any formal methods used to support their substantiations, confirm their suitability and sample outputs from them to demonstrate they have been consistently and appropriately applied.

44. The level of substantiation evidence outlined above is the minimum level of evidence that an inspector should expect to see for tasks at each level of importance. As the importance of a TINS increases, it is expected that additional analysis will be undertaken and evidence added to provide a more rigorous demonstration of the ability of the task to deliver its linked security function In addition, dutyholders may use a higher level of evidence than that suggested for all TINS, e.g. used evidence from exercises or operational experience as well as demonstrate compliance with standards for a TINS for which level 1 evidence is considered to be appropriate if they choose.
As stated above, ONR does not prescribe a specific set of factors that should be taken into account by a dutyholder when deciding on how any task important to nuclear security should be substantiated. Inspectors should, however, expect dutyholders to take a structured, systematic and proportionate approach to this, and to be able to demonstrate the adequacy of their process. Appendix 1 provides a guide for inspectors on how factors related to the importance of a security measure, the contribution of the TINS, and the task factors (such as complexity, novelty and difficulty) could be combined to determine the type of evidence needed to provide a proportionate substantiation. This provides one example of a structured and systematic process to achieve this, it is not intended to provide a model that dutyholders should adopt.

45. Application of the methods should allow the dutyholder to demonstrate that tasks assigned to humans to deliver or support nuclear security functions are feasible and achievable, minimising the likelihood that security functions will not be delivered as a result of human failure. The output from the human reliability analysis should also demonstrate that any shortfalls in the design are considered and improvements implemented, where reasonably practicable. These may include changes to the design of the task, changes to the allocation of function or improvements to performance influencing factors such as staffing and competence arrangements, procedures, equipment and

Human Machine Interfaces (HMIs). Further guidance on each of these key performance influencing factors is provided in the TAGs supporting the following SyDPs:

- SyDP 3.2 Sufficiency and Competence of Personnel Delivering Security
- SyDP 3.3 Workspaces, Equipment and User Interfaces.
- SyDP 3.4 Procedures and Administrative Controls.

46. ONR expects that substantiation evidence is provide as part of the dutyholder's security plan or supporting documentation.

47. Inspectors should consider:

- Does the dutyholder employ a suitable range of different types of evidence to substantiate the feasibility and reliability of TINS?
- Is the dutyholder's use of evidence to substantiate TINS proportionate to the relative importance, of the task for achieving the required security outcome?

References

[1] H.M. Government, “The Nuclear Industries Security Regulations 2003 (NISR) (2003/403),” 2003.

[2] ONR, “Security Assessment Principles for the Civil Nuclear Industry,” 2017.

[3] H.M. Government, “Government Functional Standard GovS 007: Security,” [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/903904/Government_Security_Standard.pdf.

[4] ONR, “ONR-CNSS-POL-001 - NISR 2013 Classification Policy for the Civl Nuclear Industry”.

[5] IAEA, “Convention on the Physical Protection of Nuclear Material (CPPNM)”.

[6] IAEA, “Nuclear Security Series No. 20. Objective and Essential Elements of a State’s Nuclear Security Regime”.

[7] IAEA, “Nuclear Security Series No. 13. Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5),” 2011.

[8] ONR, “CNS-TAST-GD-6.3: Physical Protection Systems”.

[9] ONR, “CNS-TAST-GD-11.4.5: Functional Categorisation and Classification of Security Structures, Systems and Components”.

Glossary and Abbreviations

CCTV	Closed Circuit Television
COTS	Commercial Off the Shelf
CPPNM	Convention on the Physical Protection of Nuclear Material
CPS	Cyber Protection System
CS&IA	Cyber Security and Information Assurance
EMIT	Examination Maintenance Inspection and Test
FAT	Factory Acceptance Testing
FSyP	Fundamental Security Principle
HMI	Human Machine Interface
HTA	Hierarchical Task Analysis
IAEA	International Atomic Energy Agency
KSyPP	Key Security Plan Principle
NISR	Nuclear Industries Security Regulations
NM	Nuclear Material
NSS	Nuclear Security Series
ONR	Office for Nuclear Regulation
ORM	Other Radioactive Material
PIF	Performance Influencing Factor
PPS	Physical Protection System
PSF	Performance Shaping Factor
SME	Subject Matter Expert
SNI	Sensitive Nuclear Information
SPF	Security Policy Framework
SQEP	Suitably Qualified and Experienced
SyAP	Security Assessment Principle
SyDP	Security Delivery Principle
SySSC	Security System Structure or Component
TAG	Technical Assessment Guide
TINS	Task Important to Nuclear Security

Appendix 1: Further Guidance on Proportionate Human Factors Analysis

1. This Appendix illustrates one possible approach that Dutyholders might adopt when deciding how to substantiate different Tasks Important to Nuclear Security (TINS) that make up their protective security arrangements.
It assumes that the dutyholder has adopted a system akin to that described by KSyPP 5 for functional categorisation and classification. It should be noted that Dutyholders can use alternative approaches if preferred but should be able to articulate the basis for the approach and associated decision making and demonstrate that the approach taken is structured, systematic, and delivers proportionate analysis and evidence.

2. The judgement of the level of substantiation required for a TINS is determined by:

   - the category of the Security Function it delivers or supports,
   - the classification of Security Measures necessary to deliver the security function and
   - the classification of the TINS that contribute to the security measure

3. Determination of the class of security measures is summarised in Figure 2.

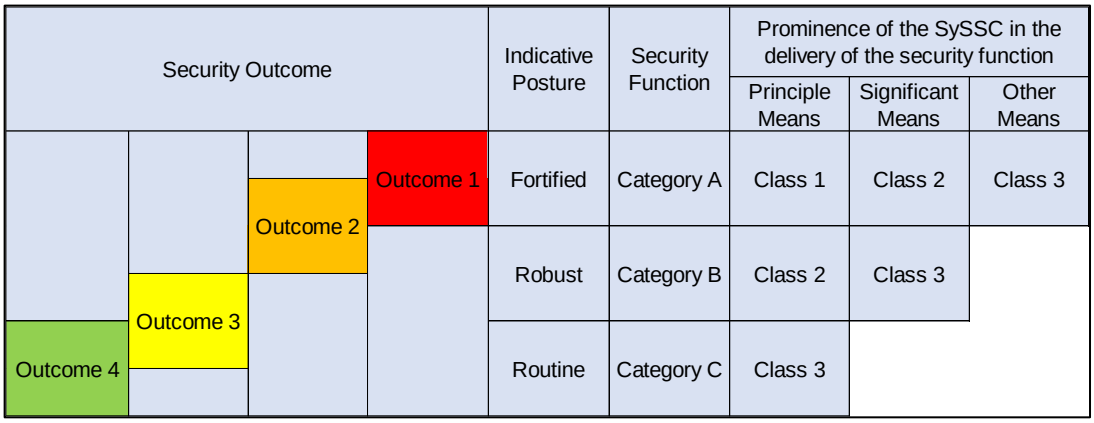

Figure 2: Security, functions and class of Security Measures

4. The level of substantiation can be determined using the following process:

   - Determine the category of the Security Function. This should be derived based on the dutyholder's categorisation for theft and sabotage and the nuclear Security Outcome that needs to be achieved. For example, an Outcome 1 facility would generally require Category A to be assigned for all Security Functions at each barrier (as defined in Annex C of SyAPs) but for other Security Outcomes a mix of categories could be assigned to individual Security Functions at the barriers. This is reflected in the range

of security postures that are shown in Annex C of SyAPs. This process is described in CNS-TAST-GD 11.4.5 [9].

- Identify all of the security measures (SySCCs and TINS) that deliver each of the security functions and then classify those measures. Security control measures can be passive engineered, active engineered or procedural/administrative and are likely to comprise a mixture of Security Structures Systems and Components (SySSCs) as well as TINS. Classification of a security measure is dependent on the importance of the security measure for achievement of the security function. Detailed advice on the categorisation of nuclear security functions and classification of security measures is provided in CNS-TAST-GD 11.4.5 [9].

- Classify each TINS that delivers or supports the achievement of the security function. In the case of security measures that are wholly operational, the class of at least one of the human tasks will be the same as the class assigned to the security measure. Where human tasks combine with a passive or active engineered control to deliver a security function, the classification of the task will be determined by how important the task is to the achievement of the function. For example, where a task is to detect an alarm linked to a Perimeter Intruder Detector System (PIDS), the classification of the task is likely to be the same as that assigned to the PISD as response to the alarm is likely to be critical for achievement of the Function. In contrast, the classification of PIDS maintenance tasks may be at a lower classification than that of the PIDS (or even unclassified) if a functional test is performed that demonstrates functioning post maintenance. This test would, most likely, be classified at the same level as the PIDS.

- Once the importance (classification) of the human task has been determined, a base level of analysis and substantiation evidence to be provided in the Security Plan can be identified. Three levels of analysis and substantiation evidence are identified, these are:

    - Level 1 – Analysis and evidence to demonstrate that human factors is appropriately integrated into the design of the TINS and that human aspects of the related system design are consistent with Relevant Good Practice (RGP) in the form of relevant codes, standards and guidance. This would be the minimum level of analysis and evidence expected to be provided in the dutyholder's security plan for a class 3 task.

    - Level 2 – Analysis and evidence from exercises and operational performance feedback that human tasks required to deliver security functions can be completed effectively and reliably. Evidence should also demonstrate that where performance weaknesses are identified in relation to the task, that reasonably practicable improvements have been sought. This builds on the level 1 analysis and together would be the minimum level of

analysis and evidence expected to be provided in the dutyholder's security plan for a class 2 task.

- Level 3 – Analysis and evidence from the application of systematic and structured methods, to demonstrate through analyses that tasks required to deliver security functions are feasible and that the likelihood of human failure has been identified and minimised by the design of tasks and identification, assessment and management of key performance shaping factors in order to substantiate that the Response (defined in Annex D of the SyAPs) can be shown to be achieved. This builds on level 1 and 2 analysis and would be the minimum level of analysis and evidence expected to be provided in the dutyholder's security plan for a class 1 task.

- The initial determination of the level of substantiation evidence required, based on the importance of the TINS may require adjustment based on factors associated with the nature of the task. Two broad factors can be used to refine the judgement of the level of substantiation evidence required, these are:

  - Difficulty of the task, which can be determined by issues such as:
    a. The amount of information to be processed, its complexity and the resultant mental workload.
    b. The physical demands of the task in terms of strength, dexterity, precision etc.
    c. The number of people that are involved in the task and the requirements to coordinate them.
    d. The number of tasks that need to be completed by the same group of staff in a short time period.
    e. The speed with which the task needs to be performed.
    f. Exposure to environmental stressors.
    g. Monotony.

  - Frequency or novelty of the task, this can be determined by factors such as:
    a. How often the task is performed, and whether it is new, novel or infrequently performed.
    b. If the task requires equipment to be used in a way which is different from how it is normally used.
    c. If the control has been recently added to the PPS / CPS.
    d. If the task is completed using new equipment or procedures.

- Where additional task-based factors are used to inform the selection of the level of substantiation evidence required, it is expected that this should only change the level of substantiation either up or down by 1 level.
  For example, if the initial level of substantiation was identified as level 1, but the associated tasks are both difficult and unfamiliar, then

consideration should be given to changing the level of substantiation required to level 2. Similarly, if the initial level of substantiation required is Level 3, but the tasks are simple, routine and well-practiced, then the level of evidence required might be adjusted to Level 2.

5. This section of Appendix 1 provides two examples of how proportionality decisions in relation to substantiation of TINS tasks could be produced. The example is based on consideration of a hypothetical nuclear site, which requires a PPS able to achieve a nuclear security outcome at level 1.

6. Table 1 provides output from the process for the security function delay at the site perimeter. Table 1 provides a summary of the output from the process this is followed by text to explain how the analysis and evidence level is derived for each TINS.

Table 1: Assignment of Analysis and Substantiation Level - (Delay Function Site Perimeter)

Security Function and Category	Security Measure	Security Measure Type	Class	TINS	Class	Initial Level	Difficulty	Frequency	Final Level
Delay Cat A	Double Fence with sterile zone	Passive Engineered	1	Inspection as part of guard patrol	3	1	Low	High	1
				Formal, periodic inspection	1	3	Low	Low	2
	Vehicle Barrier – rising barrier	Active Engineered	1	Maintain	3	1	Low	Low	1
				Test	1	3	Low	High (monthly)	2
	Guard force	Procedural / administrative	3	Patrol challenge	3	1	Low	High	1

Table notes:

Column 1 in the table identifies the security function to be achieved and the category assigned to it, this should be determined as part of the nuclear security risk assessment.

Column 2, lists each of the security measures claimed by the duty holder to provide the security function.

Column 3 identifies the type of measure, passive engineered, active engineered or procedural / administrative (TINS).

Column 4 assigns a class to each of the measures. In this case both of the engineered controls are identified as the primary means by which the security function delay is provided Two class 1 measures are provided as they provide delay to different forms of threat.

The SySSCs providing these measures would therefore need to meet the class requirements of each control. An additional means of achieving delay in the form of a guard force patrol between the double fence lines is employed, this provides a minor role in delivering the function and therefore is assigned as a class 3 measure.

Column 5 identifies the TINS associated with each measure. In the case of the fence and rising vehicle barrier two tasks are identified, two form of inspection for the fence and maintenance and testing tasks for the rising vehicle barrier.

Column 6 assigns a class to each of the TINS associated with the security measure.

In the example of the fence, two forms of inspection are identified. A regular inspection performed during a security patrol intended to identify gross defects in the fence.

This is considered to provide a minor role in achieving the security function and hence is assigned a low class. A more formal inspection of the fence is conducted periodically, and this is intended to spot defects before the function of the fence is significantly compromised. This would be assigned a classification equivalent to that applied to the fence as it is instrumental in delivering the security function.

In the example of the vehicle barrier the two tasks are assigned a different classification. Maintenance of the vehicle barrier is assigned as class 3; this is because maintenance is a supporting task to the equipment but does not directly deliver the security function. However inadequate maintenance could result in the barrier not delivering its Function and it failing to operate when required. Testing of the barrier provides an opportunity both to test that the barrier works correctly after maintenance and also periodically between maintenance periods. Given the role of testing in detecting the ability of the barrier to achieve its security function this is assigned a higher class than maintenance (Class 1).

The security measure of the guard force is a class 3 measure, therefore the tasks provided by them, is also assigned a class of 3.

Column 7 identifies the initial analysis and evidence level required to substantiate the task, which is a direct function of the class assigned to the task

Columns 8 and 9 provide the dutyholders analysis of the level of difficulty and frequency of performance of the task. An inspector should expect the dutyholder to explain the basis of the judgements made in relation to these factors.

Column 10 provides the final judgement of the level of analysis and evidence required and any adjustment to that assigned at Column 7. In the example above the dutyholder has initially assigned the need for level 3 evidence for the periodic inspection of the fence and testing of rising vehicle barrier, however, on the basis of assessment of the difficulty and frequency of the tasks, the level of analysis and evidence has been reduced to level 2. In such cases it would be for the inspector to judge that such an adjustment is appropriate.

A final column (not shown) could be used to explain the rationale of the choices made.

Table 2: Assignment of Analysis and Substantiation Level - (Insider Threat Function Site Inner Area)

Security Function and Category	Security Measure	Security Measure Type	Class	TINS	Class	Initial Level	Difficulty	Frequency	Final Level
Insider Threat Cat A	Vetting and aftercare	Procedural / Administrative	1	Assessed generically under FSyP 8					
	Security Culture	Procedural / Administrative	2	Assessed generically under FSyP 2					
	Door post contamination detection alarms	Active Engineered	3	Alarm response	3	1	low	low	1
				EIMT	3	1	low	low	1
	Search	Procedural / Administrative	3	wand search	3	1	high	high	2
	Bag Search	Active Engineered	3	Review X-Ray image	3	1	high	high	2

Table notes:

In this example the security function of insider threat mitigation is identified as a category A function. The primary means of protecting against insider threat is claimed by the dutyholder to be provided by their vetting and aftercare process which would be identified as a class 1 administrative control. The dutyholder may identify that this measure is assessed separately under FSyP 8. In such cases the inspector should seek evidence that the vetting and aftercare system is working effectively, it would be unlikely however, that an administrative control of this type would be subject to detailed human factors analysis such as that described as Level 3 analysis and evidence.

Security culture is identified in the example as the dutyholder's secondary measure to provide the security function of insider threat mitigation. This again is a type of Measure that would be addressed generically under FSyP 2 and would not be subject to detailed task based human factors assessment under FSyP 3.

The remaining security measures are all identified as class 3 measures. The first of these is door post contamination monitors used to detect the removal of NM or ORM from the inner area. The response to the alarm linked to the monitor and EIMT of the monitors are identified as

class three tasks, both of which have low difficulty and are conducted with low frequency. An initial analysis and evidence level of 1 is not adjusted based on the assessment.

The remaining security measures are two forms of search, a manual pat down search conducted by the guard force and an X-ray bag search. Both measures are aimed at detecting the introduction or removal of prohibited items. The manual search is procedural and the X-ray search hybrid involving both a human and an engineered component. Given both measures are class 3, the initial analysis and evidence requirement is level 1. However, in this case the dutyholder has identified the tasks to be difficult, this could be on the basis of OPEX including evidence of failed searches or based on reports of difficulty of the task by members of the guard force. In both cases the dutyholder has increased the level of analysis and evidence required to level 2.

These examples are provided to give an example of a method for how the level of analysis and substantiation of human based tasks could be determined. It is consistent with guidance provided in the SyAPs related to KSyPP 5 and the advice provided on Categorisation and Classification of SySSCs in TAG 11.4.5 [9]. It is not intended to be prescriptive and dutyholders should be encouraged to develop a structured and systematic method that best suits their own undertaking and arrangements for the conduct of nuclear security risk assessment.

Appendix 2: Further Guidance on Qualitative Human Reliability Analysis

Introduction

1. This appendix provides high level guidance on the application of qualitative human reliability analysis methods in the context of nuclear security. It covers four areas:

   - Task Analysis.
   - Allocation of Function.
   - Human Failure Analysis
   - Assessment of Performance Influencing Factors.

Task Analysis

2. Task analysis is the process by which a dutyholder demonstrates they understand the tasks that are required to maintain security. The analysis should consider how tasks are undertaken, the requirements they place on personnel and how well these requirements are met by the task design, equipment and operational support provided to personnel (for example via training and procedures). There are a number of formal methods that may be employed; each differs in terms of its purpose, complexity and amount of resource needed for its application. Inspectors should evaluate the adequacy of the dutyholder's approach to the analysis of tasks important to nuclear security. As part of this, Inspectors should consider how aspects such as the difficulty importance and frequency of task performance is used by dutyholders to determine which task analysis methods are employed.
   The main task analysis techniques likely to be applied in the security context are described briefly below, more detailed guidance can be found in [8].

Job Analysis / Job Task Analysis / Job Competency Analysis

3. These techniques are most commonly used as part of the Analysis phase of the Systematic Approach to Training. Job analysis is a systematic technique used to obtain a task or activity list for a specific role, this task list is then commonly assessed to identify the generic competencies required for each task. Job analysis is most commonly undertaken as a table-top exercise by training or human factors professionals supported by Subject Matter Experts (SMEs) who can provide information on the tasks associated with their roles. Job analysis is often supported and validated by documentation such as role profiles and security operating and emergency procedures.

4. Job analysis is the most basic form of task analysis and is a fundamental component of good competency management and training development and links closely to SyDP 3.2. ONR considers that job analysis provides a basis for the demonstration that security important tasks are systematically identified and a form of analysis that allows judgements on the effective delivery of tasks. This is likely to be suitable for tasks that are role based, that are familiar, frequently performed and not considered to be complex. It also forms the starting point for tasks which require further analysis using the approaches set out below.

Hierarchical Task Analysis (HTA)

5. HTA is a decomposition task analysis method. Its primary purpose is to break an overall task goal into a series of sub tasks at increasing levels of decomposition. HTA is particularly useful for the design of new tasks and to understand how existing complex tasks are completed. The technique provides a powerful basis from which to determine the order in which sub tasks should be performed in order to increase the likelihood that a task will be completed successfully.

6. An HTA can be produced from a walkdown of a task, a table-top exercise or from review of documentation such as operating procedures. Walkdown or table-top exercises are the preferred method as a procedure may not represent the best or actual way in which a task is completed. HTA is typically supported by other task analysis methods with the output from the HTA being used an input to these. HTA is a recognised tool for gaining understanding of how tasks are performed and is often used as a basis for the development of procedures and instructions and as such is linked to the requirements of SyDP 3.4.

Tabular Task Analysis

7. Tabular Task Analysis is a flexible method of task analysis that can be used to support a number of activities including task design, the development of workspaces, equipment and human machine interfaces (SyDP 3.3), and, with particular relevance to SyDP 3.1, demonstrating that tasks can be undertaken effectively and reliably.

8. Tabular Task Analysis presents information about a task in a tabular format. The rows of the table are the individual task steps, the columns of the table represent the types of information about which information is needed. This can be information about how the task is completed in terms of cues to action, information needed to make decisions, controls used to complete tasks and signals used to provide feedback on the tasks. Alternatively, the columns can collect information on performance influencing factors such as who performs a task, the procedure that guides the task and the quality of the equipment or interfaces used.

9. Tabular task analysis can also be used to support human failure assessment. Here the table columns collect information on factors such as, the type of failure that might occur, the consequence of the failure, safeguards or recovery factors that would prevent a consequence following from a failure.

Timeline Analysis

10. Timeline analysis is used to examine time critical tasks, to determine if all elements of the task can be completed in the time available. The technique plots a graph of the elapsed time on one axis with the task steps on the other axis. Task steps are derived from a HTA, and time data are either provided by SME estimates or collected via exercises. The technique should be used where time critical security functions are to be delivered by humans and it is not readily apparent that the tasks required to achieve the security function can be completed in the time available.

11. Timeline analysis can also be used to identify the numbers of personnel required to complete a task and can be used to aid task redesign by distributing tasks differently amongst personnel in situations where the time required exceeds or is close to the available time for achieving a security function. Timeline analysis can be used to support estimates of required staffing numbers to respond to an event and as such can be of benefit in demonstrating the availability of sufficient competent personnel as required by SyDP 3.2 and can also be used to assess workload demands on staff identifying periods of peak workload and their durations.

Link Analysis

12. Link Analysis is used to understand how workspaces, human machine interfaces and communication networks are used to achieve tasks.
The principal goal of the technique is to map the inter-relationships between different areas of a workspace, interface or communication network in order to ensure their design minimises the likelihood for error and enhances task performance.

13. Whilst link analysis is primarily used to support design of workspaces and interfaces and hence is most closely linked to SyDP 3.3, it can also be used to evaluate the design of an existing system to demonstrate that operators are adequately supported to achieve the tasks that are assigned to them.

Task Analysis Key Questions

14. Has a proportionate task analysis, using appropriate methods, been undertaken to substantiate that tasks important to security have been designed to match human capabilities and limitations?

15. Is design of workspaces, equipment, training and procedures underpinned by suitable and sufficient task analysis?

Allocation of Function

16. The primary aim of the analysis of tasks undertaken under SyDP 3.1 is to demonstrate that where tasks important to nuclear security are allocated to humans, this allocation is justified on the basis of a match between human capabilities and the demands of the task. The process by which tasks are allocated to a human, an engineered system or an appropriately designed mix of the two, is referred to as Allocation of Function. The allocation of function decisions should reflect an understanding of the relative strengths and limitations of humans and use engineering systems to complement human abilities. Consideration of human abilities should encompass cognitive, physiological and physical aspects.

17. Humans are good at carrying out relatively varied work, while machines can process vast quantities of information and be used to complete more boring or predictable tasks. For example, intelligent detection systems (e.g., fence or door alarms) are often used in CCTV rooms to replace continuous human monitoring and automatically detect intruders or other events; alarms (auditory or visual) are often linked to these systems.

18. Use of these systems should be very carefully considered in the context of other tasks that operators need to carry out, the main question being – is detection actually enhanced by such devices?

19. Making certain processes automatic can help to reduce the burden on operators but it is important that operators can override such automation for more unusual operating conditions and where decision making is required. In addition, in practice it may not always be the case that the workload of operators is actually reduced, especially if systems are unreliable or generate an unacceptable level of false positive, or false negative, alarms. Dutyholders should give consideration to these aspects as part of their system design.

20. As well as considering the allocation of individual tasks, it is necessary that an analysis of the overall allocation of security tasks to personnel is made in order to demonstrate that there is not an over reliance on the human component to deliver security functions. It should be demonstrated that a balanced approach to security is provided in which human and engineered components of the system work together to achieve high levels of security performance. This is important to ensure that the overall task design provides a meaningful job role for the human in order to maintain motivation and provide job satisfaction.

Allocation of Function Key Questions

21. Are decisions for allocation of tasks important to security between people and engineered systems underpinned by a structured and systematic analysis process?

22. Is the allocation of function compatible with human physical and psychological capabilities?

23. Does the totality of tasks assigned to a human when carried out under the worst possible conditions allow him to maintain an adequate level of performance? Allocation should consider the whole of the job rather than individual tasks and responsibilities.

24. Are negative impacts of automation, e.g., overreliance on automation, loss of situational awareness, long periods of inactivity and boredom considered in the allocation of function analysis?

25. Is the human's role in detecting failure of automation considered and does the system design allow for the operator to adopt manual control in such situations?

Human Failure Analysis

26. When identifying human failure for tasks important to nuclear security dutyholders should consider the different ways in which humans may fail to successfully complete a task and focus on those particular failures which would mean a security function is not delivered. Three broad classes of human failure can be identified, human errors, violations and malicious insider acts all of which should be considered in the dutyholder's human failure analysis.

27. Considering human error, at the simplest level, a distinction can be made between errors of omission, where a person fails to perform a task or key step and errors of commission, where they perform a task or key step incorrectly. Errors of commission take many forms and have numerous causes. Examples of errors of commission include:

    - Performing the right action on the wrong object, e.g., checking the image on the wrong CCTV monitor.
    - Performing the wrong action on the right object e.g., Checking the issue rather than expiry date on an access pass.
    - Performing an activity for too long or short a period, e.g., focussing on a CCTV for too long or short a time.
    - Performing an action with too much or too little force.
    - Performing task steps in the wrong order.
    - Collecting or recording the wrong information.
    - Misinterpreting a situation and taking the wrong course of action, e.g., failing to correctly classify a document containing sensitive nuclear information.

28. A further human failure type, violation, should also be considered as part of the human failure analysis. A violation is a deliberate deviation from a rule or procedure, often in the form of a short cut, which the person believes will have no negative impact on security. An example may be failing to secure a store containing nuclear material because an item is only removed from it for a short period of time.

29. Malicious acts i.e., a deliberate attempt to circumvent a security system are not normally considered by human reliability analysis, however, threats of this sort from external actors and insiders are a necessary component of a security risk analysis. Dutyholders should demonstrate how tasks are designed to protect against the insider threat as part of their approach to human failure analysis.

30. Where the human failures assessment identifies task success and the achievement of security functions are vulnerable to human failure, the assessment should also identify features of the task that are intended to safeguard against (prevent) or recover (allow the failure to be detected) the failure and evaluate the strength of these safeguards and recovery features.

31. In some settings, e.g., nuclear safety, human reliability analysis is used to derive quantitative estimates of task reliability or error likelihood. ONR does not expect such quantitative approaches to be used in the analysis of security tasks.

Human Failure Analysis Key Questions

32. Does the human failures analysis provide sufficient evidence that security tasks undertaken by humans have been designed such that the likelihood of human failures is minimised?

33. Does the assessment of human tasks important for nuclear security include consideration of a suitable range of human failure types including errors, violations and malicious acts?

34. Does the human failure assessment identify and evaluate the likely effectiveness of safeguard and recovery factors?

Assessment of Performance Influencing Factors

35. Evaluating and improving Performance Influencing Factors (PIFs) is the primary approach for maximising human reliability and minimising failures. PIFs are the characteristics of people, tasks and organisations that influence human performance and therefore the likelihood of human failure. Key PIFs that impact human performance in relation to security are addressed by the SyDPs underpinning FSyP 3 and include workload, staffing, competence and training, design of workspaces, equipment and human machine interfaces as well as procedures. Further guidance on each of these key performance influencing factors is provided in the TAGs supporting the following SyDPs:

- SyDP 3.2 Sufficiency and Competence of Personnel Delivering Security
- SyDP 3.3 Workspaces, Equipment and User Interfaces.
- SyDP 3.4 Procedures and Administrative Controls.

Assessment of Performance Influencing Factors Key Questions

36. Does the qualitative human reliability analysis include consideration of the effect of PIFs?

37. Have all PIFs specifically relevant to each task been identified and are judgements of the adequacy of their design appropriate?

38. Where the assessment of a PIF is negative have improvements been identified and implemented in order to improve reliability of human performance?