Functional Categorisation and Classification of Security Structures, Systems and Components			
Doc. Type	ONR Technical Assessment Guide (TAG)		
Unique Doc. ID:	CNS-TAST-GD-11.4.5	**Issue No.:**	1
Record Reference:	2022/17825		
Date Issued:	Apr-22	**Next Major Review Date:**	Apr-27
Prepared by:		Superintending Inspector	
Approved by:		Superintending Inspector	
Professional Lead:		Superintending Inspector	
Revision Commentary:	First Edition		

Table of Contents

1. Introduction 3

2. Purpose and Scope 4

3. Relationship to Relevant UK Legislation and Policy 5

4. Relationship to International Standards and Guidance 7

5. Advice to Inspectors 8

6. Regulatory Expectation 9

7. Key Security Plan Principles 10

8. Security Functions and Categorisation 11

9. Security Classification of Structures, Systems and Components 15

10. Additional Features to Consider in Categorisation and Classification 20

References 22

Glossary and Abbreviations 23

Appendix 1: Table Showing Security Outcome, Security Functions Categorisation and SySSC Classification Linkage 24

Appendix 2: Demonstration of Categorisation and Classification of SySSCs at a Hypothetical Facility 25

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 2003') (reference [1]) may also use the 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 the exercise of their regulatory judgment during intervention activities relating to the assessment of a dutyholder's arrangements for the categorisation of security functions and the classification of Structures, Systems and Components (SSCs) which form elements of the security protective system. It aims to provide general advice and guidance to ONR inspectors on how to assess this aspect of a dutyholder's security arrangements. It does not set out how ONR regulates the dutyholder's arrangements. It does not prescribe the detail, or methodologies for dutyholders to follow to demonstrate they have addressed the SyAPs. It is the dutyholder's responsibility to determine and describe this detail within their submission and for ONR to assess whether the arrangements are adequate.

4. Safety SSCs such as computer-based safety systems should already have been subject to a scheme of safety categorisation and classification which follows a similar methodology and achieves much the same aim as this TAG (NS-TAST-GD-094 [3]). Whilst certain SSCs may have both safety and security purposes, it may not be necessary to assign separate categorisations and classifications for each purpose. The scope of this TAG is focused on nuclear security SSCs but may also be relevant to other SSCs where a safety categorisation and classification is not applicable.

3. Relationship to Relevant UK Legislation and Policy

5. 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.

6. 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.

7. 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 that they have effective processes in place to achieve Key Security Plan Principles: 5.1 – Security Categorisation, and 5.2 Security Classification. The TAG is consistent with other TAGs and associated guidance and policy documentation.

8. The Government Functional Standard on security [4] 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 the 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.

9. The Government Security Classifications document, together with the ONR Classification Policy [5] describes 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.

10. Whilst it adopts a simpler methodology, this TAG is consistent with the principles in nuclear safety assessment TAG for categorisation and classification [3].

11. This TAG is also related to NS-TAST-GD-003 [6] which provides further detail on the difference between safety related systems and safety systems, and their design expectations.

4. Relationship to International Standards and Guidance

12. The essential elements of a national nuclear security regime are set out in the Convention on the Physical Protection of Nuclear Material (CPPNM) [7] and the IAEA Nuclear Security Fundamentals [8]. Further guidance is available within IAEA Technical Guidance and Implementing Guides.

13. A more detailed description of the elements is provided in Recommendations-level guidance, specifically Nuclear Security Series (NSS) 13 [9].
This document defines a number of fundamental principles. Fundamental Principle H concerns the graded approach, it states that:

> ‘Physical protection requirements should be based on a graded approach, taking into account the current evaluation of the threat, the relative attractiveness, the nature of the nuclear material and potential consequences associated with the unauthorized removal of nuclear material and with the sabotage against nuclear material or nuclear facilities.’

14. Therefore, a graded approach is used to provide higher levels of protection against events that could result in higher consequences.

15. Fundamental Principle I is Defence in Depth. This principle states that:

> ‘The State’s requirements for physical protection should reflect a concept of several layers and methods of protection (structural, other technical, personnel and organisational) that have to be overcome or circumvented by an adversary in order to achieve his objectives.’

16. Within this TAG, these methods of protection are referred to as SySSCs.

17. NSS 13 [9] then combines these principles by stating that:

> ‘The three physical protection functions of detection, delay and response should each use defence in depth and apply a graded approach to provide appropriate protection.’

18. This TAG provides guidance on how functional categorisation and classification of SySSCs can be incorporated within physical protection system design, building defence in depth, and applying the graded approach.

19. The International Atomic Energy Agency (IAEA) Safety Guide – Safety Classification of Structures, Systems and Components in Nuclear Power Plants [10] is applicable to all engineering disciplines, including those for security, and has also been considered during the development of this TAG and the guidance here is consistent with the recommendations made by the IAEA.

5. Advice to Inspectors

20. Functional categorisation and classification can be a complicated subject and it is easy to fall into an error trap of developing unworkable systems that aren't understood and don't add value. Therefore, scheme developers and assessors should always keep in the forefront of their mind the primary purpose of a categorisation and classification scheme. This purpose is to facilitate dutyholder understanding of the different components of their security arrangements in terms of how they contribute to the overall security effect and the relative importance of that contribution.

21. The end point should be a scheme that provides confidence critical SySSCs are designed with appropriate levels of performance, reliability, resilience and redundancy; are adequately tested, inspected and maintained; and are supported by robust contingency arrangements should they fail. An effective scheme will also have benefits in demonstrating that adequate defence in depth is in place, thus helping to identify and mitigate any single points of failure. Regardless of how a dutyholder approaches categorisation and classification it must take account, as appropriate, of all the components that together make up an effective security regime including, for example, human factors, workforce trustworthiness and cyber. It should also consider relevant safety SSC.

22. The term categorisation is used to apply groupings in many different contexts such as theft/sabotage consequences, radioactive sources and modifications processes. Therefore, inspectors should be aware that dutyholders may choose to adopt a different nomenclature to provide differentiation and avoid confusion. Further clarification should be sought from the dutyholder where terminology used for the principles in this TAG is unclear to the inspector.

23. Security function categorisation is the process by which the security functions, both during normal operation and in the event of an incident, are categorised based on their significance for the protection of nuclear material, other radioactive material and associated facilities. (Key Security Plan Principle (KSyPP) 5.1). These security functions should be identified by following a systematic approach and categorised according to the consequences of a successful act of theft or sabotage (i.e., directly related to the security outcome to be achieved in accordance with SyAPs OFFICIAL SENSITIVE:SNI Annex C).

24. SySSC classification is the process by which SySSCs are classified on the basis of their importance as a means of delivering the security functions (KSyPP 5.2). The class assigned to an SySSC indicates the level of confidence required in its ability to deliver its security function, and hence its contribution to the overall security outcome.

25. The definition of outcome, categorisation and classification gives a hierarchy of importance to the SySSC, which in turn defines the importance ascribed to

its design, construction/manufacture, installation and commissioning. Additionally, this importance also sets the arrangements for its operation, including maintenance and testing regimes, as well as substitution and availability requirements.

26. This guide is restricted to nuclear security function categorisation and SySSC classification; it does not address the categorisation (i.e., the security grading) of documents, plant modifications or other aspects, other than to note that any such categorisation should be informed by the security functions and SySSCs to which they relate.

6. Regulatory Expectation

27. The regulatory expectation placed upon the dutyholder is that they will ensure that the security plan identifies a systematic approach to the identification and categorisation of functions to demonstrate how the plan meets the required outcomes. The security plan will also identify a systematic approach to the identification and classification of structures, systems and components which provide these functions.

Key Security Plan Principles	Security Categorisation	KSyPP 5.1
The security functions to be delivered at a dutyholder's site and facilities, in all modes of operation, should be identified and then categorised based on their significance with regard to security.		

Key Security Plan Principles	Security Classification	KSyPP5.2
Structures, systems and components that have to deliver security functions should be identified and classified on the basis of those functions and their significance to security.		

7. Key Security Plan Principles

28. A nuclear facility should be designed and operated with layers of defence in depth that build deterrence but are designed to ensure protection in the event deterrence fails and provide mitigation should a security event occur (KSyPP 4). The identification and categorisation of security functions and the classification of SySSCs are key activities required for the successful and balanced implementation of the layers of defence in depth incorporating the graded approach.

29. The annexes to the SyAPs present indicative postures for the functions needed to deliver the security outcomes. For physical and cyber protection systems, these are in Annexes C and H respectively. Summaries of how these postures can be achieved are presented in Annexes E and J.

30. Whilst there may be subtle nuances, there is a clear relationship between the security outcome and posture of Physical Protection Systems (PPSs) with categorisation of security functions and classification of SySSCs. Appendix 1 demonstrates this relationship by providing an example framework of how a security function categorisation and SySSC classification scheme may be mapped across the PPS outcomes detailed in SyAPs Annex C.
This approach may be applied by dutyholders directly during the design of new facilities or the review of existing facilities. In both cases, the approach should be supported by a proportionate level of analysis and evidential underpinning. When doing this dutyholders must appreciate the importance of SySSC in delivering the PPS outcome relevant to their site.

31. Security function categorisation (KSyPP5.1) should be distinct from, and normally be carried out prior to, SySSC classification (KSyPP5.2).
The security function category is one of a number of criteria used in choosing and designing the SySSC and should be linked to an associated Operational Requirement.

8. Security Functions and Categorisation

8.1. Definition and Purpose of Security Functions

32. A security function is a specific purpose or objective that must be accomplished so the overall CPS/PPS outcome can be achieved. It should usually be specified or described with minimal or no reference to the means of achieving it. This provides conceptual separation of a security function from the means by which it will be delivered. This is a particularly helpful approach in the design of new plant and is also valuable for existing plant reviews and modifications.

33. The following sections describe the identification and categorisation processes expected to be defined within the dutyholder's security plan to deliver a systematic approach to identifying the importance of functions which contribute to the delivery of defined security outcomes.

8.2. Identification of Security Functions

34. The security functions are high level objectives that must be delivered to maintain nuclear security.

35. The identification of security functions should be based on an analysis of the required outcomes for the facilities based on the threats which could arise as identified through thorough adversary path analysis (including those posed by insiders). Examples of high level physical and cyber protection system security functions – as used in Annexes C and H in the SyAPs annexes - for a nuclear facility include:

- PPS Security functions
    - Delay
    - Detect
    - Assess
    - Unauthorised Access Control
    - Insider Threat Measures
- CPS security functions
    - Identify
    - Protect
    - Detect
    - Respond
    - Recover

36. These are broadly comparable to the functions defined by the IAEA. However, additional or other functions may be defined and dutyholders are encouraged to design a bespoke schema appropriate for their particular operations and PPS/CPS.

37. The high-level security functions identified above can be broken down into increasingly more detailed lower-level security functions. The dutyholder's arrangements should define the level of breakdown at which functional categorisation is applied. In general, the level of functional decomposition should continue to a level at which the roles of different security systems needed to deliver these functions can be identified. Security function categorisation applied at too high a level can result in oversimplification, mis-categorisation and the inability to differentiate the importance of different sub-functions that contribute to delivery of the higher-level function.

38. For example, the high-level security function of delay can be broken down into a number of sub-functions such as:

- Delay an on-foot attack
- Delay a vehicle attack

39. Security function categorisation would then be applied at the lowest level of decomposition and SySSCs delivering the security functions at which categorisation is applied would then be classified.

8.3. Security Function Categorisation

40. The dutyholder's categorisation scheme should:

- define the security function categories and the process through which security functions are categorised;
- employ an appropriate number of security function categories (three are recommended by IAEA guidance for safety categorisation and this may be equally appropriate for security functions, Reference 8);
- be distinct from SySSC classification to avoid confusion;
- be specific enough to enable different users to consistently assign the same categorisation to a security function;
- include appropriate flexibility to take account of unforeseen circumstances.

41. The category assigned to a security function should consider:

- the role the function plays in maintaining security during normal operations;
- The potential for a functional failure to realise a serious vulnerability.

42. As noted above, the security functions should be described separately to the engineering means by which they will be delivered. Security function categorisation, therefore, should not usually take account of redundancy,

diversity or independence within the SySSC delivering the function. For example, if it has been determined that a particular function is Category A, then the presence of multiple Class 1 systems is not grounds to reduce the category to B.

43. As inferred by the SyAPs Unifying Purpose Statement (UPS), the purpose of nuclear security is to protect the public from the risks arising from a radiological event caused by the theft and/or sabotage of Nuclear Material (NM), Other Radioactive Material (ORM) and associated facilities or through the compromise of SNI. For theft, NM is graded according to proliferation concern (i.e., the degree of ease with which the material could be used to construct a nuclear device - refer to [11]). For sabotage, NM/ORM and associated facilities are graded according to the radiological consequences based on a worst-case successful attack (refer to [12]). Lastly, SNI is graded according to its potential to facilitate proliferation or a malicious act against nuclear premises (Refer to the ONR Classification Policy). Therefore, the consequences of theft/sabotage and SNI compromise can be used to derive the importance of the PPS and associated SySSCs in maintaining nuclear security. Furthermore, given how the categorisation for theft and sabotage is used to determine the PPS outcome, there is also a clear relationship between these outcomes and security functional categorisation. Appendix 1 provides a table which demonstrates these links.

44. In light of this relationship, paragraph 4.5.1 in SyAPs presents the following recommended security functional categorisation scheme:

- Category A (SyC A) – any nuclear security function that needs to achieve Fortified posture for Outcome 1 or 2;
- Category B (SyC B) – any nuclear security function that needs to achieve Robust posture for Outcome 2 or 3;
- Category C (SyC C) – any nuclear security function that needs to achieve Routine posture for Outcome 3 or 4.

8.4. Example Categorisation Scheme

45. This section sets out an outline process that would meet regulatory expectations for security functional categorisation. ONR inspectors should view it as a starting point to inform their assessment of the suitability and sufficiency of a dutyholder's core arrangements. It is not a prescribed method and other approaches can be used. The first task, based on a vulnerability assessment, is to assign an initial expectation of a security function category using a process driven mainly by the physical and cyber protection system posture and outcome annexes (C and H) in SyAPs. Posture can be taken to align to Category (Fortified = Cat A, Robust = Cat B, Routine = Cat C).

46. The most important factors in this determination are the magnitude of the vulnerability should the security function not be performed; and the potential consequences of a successful malicious act.

47. As detailed earlier, Appendix 1 provides an example of how security functional categorisation can be mapped across SyAPs Annexes C and H to demonstrate the importance of the function and how this increases as higher levels of outcome must be achieved. However, dutyholders have flexibility to categorise functions in different ways to suit their facility, provided the plan demonstrates that the outcomes will be achieved. Intended as further indicative guidance, Appendix B provides a high-level excerpt of how categorisation of security functions and classification of SySSCs may be applied across a hypothetical nuclear facility.

48. It may be necessary to refine the initial functional category to incorporate additional considerations or factors. These factors might include aspects such as the type or form of the material being protected. For example, it might be appropriate to reduce the functional category where the nuclear material being protected is highly dilute and stored within grouted drums or vitrified waste.

49. Another consideration is the role and position of the security function in providing defence in depth. It may be appropriate, for example, to lower the category of one security function if the category associated with an alternative function is increased to compensate.

50. Inspectors should consider:

- Does the dutyholder have a systematic approach to the identification of functions which ensure the outcome is achieved?
- Does the identification scheme for functions consider all forms of the DBT including insider threats?
- Does the dutyholder have a systematic approach to the categorisation of functions?
- Does the categorisation approach clearly take account of the consequences of failure to deliver a function?
- Does the categorisation approach show how the overall outcome is achieved and take account of the indicative postures in the SyAPs annexes?
- Is the categorisation approach proportionate to the outcome to be achieved?
- Is the categorisation approach repeatable and transparent?
- Does the categorisation approach take due account of the importance of defence in depth and multi-layer barriers?

9. Security Classification of Structures, Systems and Components

9.1. Definition of Security SSC (SySSC) Classification

51. A security classification should be assigned to each SySSC that supports delivery of a security function. This is to ensure its importance in achieving that function is recognised, understood and defined. The benefit of assigning a classification early in the design process is that the rigour of the design process can match the importance of the SySSC. During operations, the SySSC will need to achieve availability, reliability and maintenance requirements as informed by the importance of its classification. Therefore, whilst it is a particularly helpful approach in the design of new plant, it is also valuable for existing plant reviews and modifications.

52. The following sections describe the identification and classification processes expected to be defined within the dutyholder's security plan to deliver a systematic approach to identifying the importance of SySSCs and their role in delivering or supporting the security functions. Dutyholders should remember that, regardless of the classification assigned to a SySSC, any SySSC that is the principal means of delivering a function must be recognised as such and given appropriate priority by the dutyholder
(e.g., reliability and resilience, EMIT etc), commensurate with its importance in delivering that function.

9.2. Identification of SySSC to Deliver Functions

53. The dutyholder's scheme for identification of SySSCs with a security function should:

- Identify those SySSCs required to maintain nuclear security; and,
- Consider human processes as well as physical and cyber systems to ensure all security measures at the premises are captured in the classification scheme.

9.3. Classification of SySSC to Deliver Functions

54. The categorisation of each security function should be used to define the required class of the security structures, systems and components that deliver the function. The dutyholder's classification scheme should:

- define the classes of SySSCs and the process for determining the way in which they are assigned;

- be used for nuclear security purposes and not used in the context of the control of any non-security aspects (e.g., workforce efficiency surveillance);
- employ an appropriate number of SySSC classes (three are recommended by IAEA guidance for safety classification and this appears equally appropriate for security measures [6]);
- be distinct from security function categorisation to avoid confusion;
- be specific enough to enable different users to consistently assign the same classification to a SySSC; and,
- include appropriate flexibility to take account of unforeseen circumstances.

55. The suggested classification scheme makes use of the three-class scheme recommended in the SyAPs section 4.5.2:

- Class 1 (SyC 1) – any structure, system or component that forms a principal means of fulfilling a Category A security function;
- Class 2 (SyC 2) – any structure, system or component that makes a significant contribution to fulfilling a Category A security function, or forms a principal means of ensuring a Category B security function;
- Class 3 (SyC 3) – any other structure, system or component contributing to a categorised security function.

9.4. SySSC Reliability and Resilience

56. The class that can be claimed for an SySSC is fundamentally linked with its reliability and resilience. For example, a higher-class detection system will have higher probability of detection and use multiple complimentary technologies to build resilience and redundancy. In that regard, a Class 1 system design expectation might incorporate microphonic and infrared sensors. This contrasts to a Class 3 system that might be predicated on routine guard force patrolling.

57. The hierarchy of control measures (refer to KSyPP 1) should ensure that passive means of protection are given greater prominence overactive systems. This in turn will result in enhanced reliability and resilience from passively engineered protective measures such as civil engineering structures including buildings and vehicle barriers.

58. It is recognised that all SySSCs used to deliver a security function will suffer faults or failures during their lifecycle. Classification of systems will aid in the development of substitution rules and compensatory measures, identify priorities for their repair, and identify the time during which the non-availability

of the system or part of it is acceptable. It may also inform funding decisions as SySSC become obsolescent.

59. As SySSC class is directly connected to resilience, it is intimately linked with the robustness of the engineering and the incorporation of high reliability design principles (such as redundancy, diversity and independence) as well as the quality of all the other activities associated with putting the SySSC into service (such as commissioning and management of concessions during installation).

60. Having identified SySSCs and assigned a class to them, the dutyholder should provide evidence that each SySSC achieves the performance requirements for the required class. This process of SySSC substantiation should demonstrate the SySSC achieve the security function and are sufficiently reliable. This process should cover the human actions required to achieve the security function (including operation, examination, maintenance inspection and test tasks).

9.5. Example SySSC Classification Scheme

61. This section sets out an outline process that would meet regulatory expectations for the classification of SySSCs. ONR inspectors should view it as a starting point to inform their assessment of the suitability and sufficiency of a dutyholder's arrangements. It is not a prescribed method and other approaches can be used.

62. The first task involves the assignment of an initial expectation of the SySSC classification using Table 1 below. The key factors in this assignment are the categorisation of a security function(s) to be performed by the item together with the prominence of the SySSC in delivery of the security function and the role in delivering the overall outcome. The dutyholder should, in the case of a new facility, design SySSCs to achieve the required class or in the case of an existing facility select candidate SySSCs and determine if they meet or can be made to meet the required class. In either case evidence should be presented to substantiate that the SySSC meets the required class.

63. The main expectation is that the principal means/first line of providing a security function takes its classification based directly from the category of security function: Class 1 for Category A, Class 2 for Category B and Class 3 for Category C. Should they be necessary, any SySSCs assigned as a backup measure or providing defence in depth may then step-down to the next lower class in line with the Table. If two means of providing a security function are identified, then one of them should normally be identified as the principal means. It is not normally appropriate to identify both systems only as significant means. For example, a Category B function should be delivered principally by a Class 2 system and the fact that there may be two systems delivering the function is normally insufficient grounds to justify both as Class 3. Any SySSC that is the principal means of delivering a function must be recognised as such and given appropriate priority by the dutyholder (e.g.,

reliability and resilience, EMIT etc), commensurate with its importance in delivering that function.

Table 1: Initial SySSC classification

		Prominence of the SySSC in the delivery of the security function		
		Principal means	Significant means	Other means
Security function	Category A	Class 1	Class 2	Class 3
	Category B	Class 2	Class 3	
	Category C	Class 3		

64. As a single SySSC may contribute to the delivery of a number of security functions, its required class should be determined by the highest category function that it is intended to deliver.

65. Following the initial classification, it may be necessary to incorporate a number of other factors. As with categorisation, this outline classification scheme does not provide detailed guidance and the factors identified below should be seen as examples for further understanding of the dutyholder's own arrangements.

66. One factor is to ensure that a security system or security-related system is not undermined by a lower classification auxiliary service or other support feature, such as back-up power supplies. Auxiliary services that support components of a security or security-related system should be considered part of that system and should be classified accordingly unless their failure does not prejudice successful delivery of its security function.

67. A further factor is the importance of the SySSC in maintaining protection or restoring control of the site to allow the safety systems to be re-established during or following a security event.

68. Inspectors should consider:

- Does the dutyholder have a systematic approach to the identification of SySSCs which support delivery of the categorised security functions?
- Does the dutyholder have a systematic approach to the classification of SySSCs which support the delivery of functions?
- Does the classification approach align (Table 1) with the required function, and justify those SySSCs which do not?
- Does the classification approach apply to supporting and sub-systems as well as the main security SySSCs?

- Is the classification approach proportionate to the outcome to be achieved?
- Is the classification approach repeatable and transparent?
- Does the categorisation approach take due account of the importance of defence in depth and multi-layer barriers?
- Is the classification of an SySSC reflected in its substitution, availability and maintenance requirements?
- Is the classification of an SySSC reflected in its design standards, codes and justification?

10. Additional Features to Consider in Categorisation and Classification

10.1. Number and Quality of Security Systems

69. There are no fixed requirements as to the number of security systems required to deliver a security function. A single Class 1 security system, for example, might be suitable and sufficient in providing a Category A security function in some circumstances; on the other hand, a Class 1 security system backed-up by a Class 2 system may be required, particularly for systems which need a high degree of reliability in a wide variety of environmental conditions (snow, rain, sunshine) and are a key component in delivery of a security function.

70. Once the required category for each function has been determined, the SySSCs that achieve the security function should be identified. These may be already present in an existing facility or be specified in the design of a planned one. One of the SySSCs should be selected as the principal means of achieving the function and this should be assigned the highest applicable SySSC class according to Table 1 above. If other SySSCs are required to achieve the security function performance requirements these should be identified as the secondary and tertiary SSCs and classified accordingly. Once all the SySSCs required to achieve a security function have been identified, these should be assessed to substantiate that they meet the required effect defined in Annex D of the SyAPs for each security function.

71. In summary, the required class of the primary SySSC for each function can be determined using Appendix A below in conjunction with SyAPs Annex C. The claimed SySSCs must achieve the response defined in Annex D of the SyAPs for each security function.

72. The dutyholder should demonstrate that the identified SySSC(s) achieve the required response through for example; analysis, modelling, simulation or a combination of them as part of vulnerability assessment.

10.2. Combining Systems and Security Cases

73. As indicated earlier in this TAG, it is not normally acceptable to replace a higher classification system with multiple lower-class systems, e.g., to replace a Class 1 system with two Class 2 systems. Where this is unavoidable (e.g., where alternative means of achieving the required functionality and / or security performance are not readily available), the recommended approach would be to consider the multiple lower-class systems as a whole and demonstrate that in combination they achieve the integrity of the original higher-class system that is being replaced. In such instances there may be a need to recognise both the individual classification and the higher collective classification. This is particularly relevant to security systems which address

insider threats where no single form of protective measure will give full protection against the threat, even for the highest outcome requirements.

74. Considering separate systems in combination as a single classified system may also be preferable when there are similarities in location or function such that they are vulnerable to common cause failures.

10.3. Security Measures and Human Factors

75. The term security measure is used to encompass both the SySSCs and Tasks Important to Nuclear Security (TINS), the human actions needed to deliver security functions. A security measure is defined as a security system, or a combination of procedures, operator actions and security systems that protects against an incident. Security measures should be identified against the delivery of the security functions at all levels that contribute towards providing defence in depth.

76. Where security functions are delivered or supported by human action, these human actions should be identified, classified and substantiated. Further guidance on a potentially suitable methodology for the categorisation and classification of human actions can be found within [13].

77. Inspectors should consider:

- Are operator actions and processes suitably classified and categorised?
- Is the classification of an SySSC commensurate with its substitution and availability requirements?
- Is the classification of an SySSC commensurate with its design standards, codes and justification?
- Are combinations of SySSCs considered appropriately?

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] ONR, “NS-TAST-GD-094 - Categorisaiton of Safety Functions and Classification of Structures (2020/262117)”.

[4] 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.

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

[6] ONR, “NS-TAST-GD-003 - Safety Systems”.

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

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

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

[10] IAEA, “IAEA Safety Standards - SSG-30 - Safety Classification of Structures, Systems and Components in Nuclear Power Plants,” 2014. [Online]. Available: https://www.iaea.org/publications/10555/safety-classification-of-structures-systems-and-components-in-nuclear-power-plants.

[11] ONR, “CNS-TAST-GD-6.1 - Target Identification for Theft”.

[12] ONR, “CNS-TAST-GD-6.2 - Categorisation for Sabotage”.

[13] ONR, “CNS-TAST-GD-3.1 Identification and Analysis of Security Tasks and Roles”.

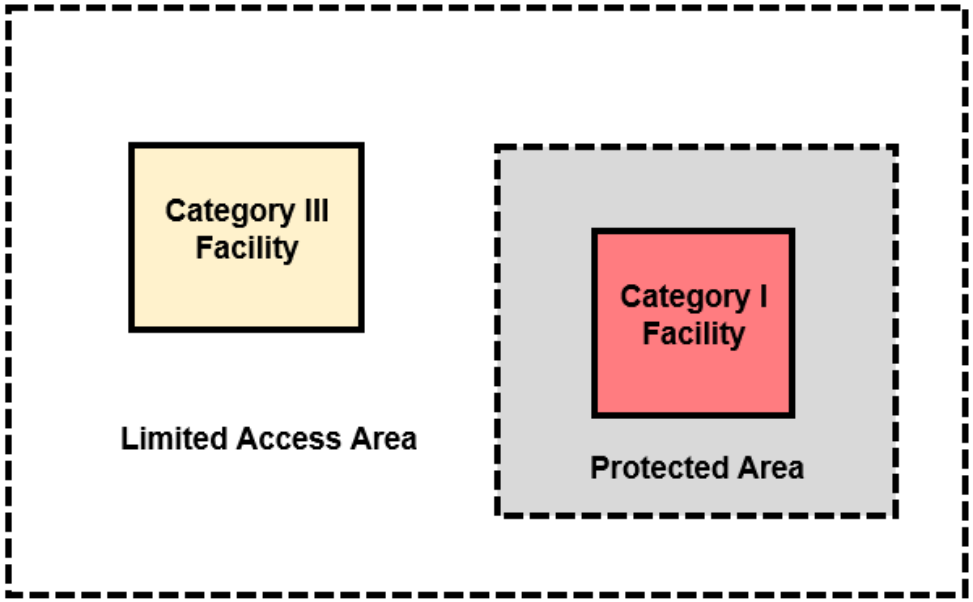
Glossary and Abbreviations

CCTV	Closed Circuit Television
CPS	Cyber Protection System
DBT	Design Basis Threat
IAEA	International Atomic Energy Agency
KSyPP	Key Security Plan Principle
NISR	Nuclear Industries Security Regulations
NM	Nuclear Material
NSS	(IAEA) Nuclear Security Series
ONR	Office for Nuclear Regulation
ORM	Other Radioactive Material
SNI	Sensitive Nuclear Information
SySSC	Security Structure, System or Component
SyAP	Security Assessment Principle
SyC	Security Categorisation (letter), Classification (number)
TAG	Technical Assessment Guide
TINS	Task Important to Nuclear Security

Appendix 1: Table Showing Security Outcome, Security Functions Categorisation and SySSC Classification Linkage

Security Outcome	Indicative posture	Security function	Prominence of the SySSC in the delivery of the security function		
			Principal means[1]	Significant means	Other means
Outcome 1	Fortified	Category A	Class 1	Class 2	Class 3
Outcome 2	Robust	Category B	Class 2	Class 3	
Outcome 3	Routine	Category C	Class 3		
Outcome 4					

Appendix 2: Demonstration of Categorisation and Classification of SySSCs at a Hypothetical Facility



Area	Function	Sub Function	Category	Claimed SySSC		
				Class 1	Class 2	Class 3
Limited Access Area	Delay	Delay Pedestrian	A	Inner ENHANCED 2 EP rated fence with barbed Tape Obstacles in sterile zone	Outer BASE 1 EP rated fence	Anti-intruder foliage to exterior of site fence
				Enhanced EP 2 Pedestrian turnstile		
				Staffed EP 2 Gate		
		Delay vehicle	A	PAS 68/69 vehicle barrier integrated into the outer fence		
				PAS 68/69 Inner vehicle gate	Outer vehicle gate	Traffic calming entry road design
	Detect		A	Dual knock PIDS using independent infrared and microwave technologies monitored 24/7 in SSCR	Guard force patrolling Monitored PTZ cameras	Staff observation and reporting of suspicious activity
	Assess		A	Fixed line CCTV covering sterile zone with 24/7 CCTV monitoring of alarms in SSCR	Routine guard force and armed response force patrolling	Staff observation and reporting of suspicious activity

					Monitored PTZ cameras	
	Access Control		B		Pass activated Enhanced 2 EP turnstile, Rising arm vehicle barrier Guard force pass checks on ENHANCED 2 EP gate	
	Insider Threat Measures		B		100% visitor searching access and egress 10% Staff Access search 5% Staff exit search	Staff reporting suspicious or unusual behaviour
	Response		A	Onsite Armed Response Force	Onsite guard force Situational Awareness Surveillance Drones Radiocommunications	Offsite response
Protected Area/ Cat I Facility	Delay		A	NM store constructed to ENHANCED 20 BF	Building fabric to ENHANCED 10 BF	ENHANCED 2 EP protected area fence
	Detect		A	Vibration detection on building and store wall fabric	Microphonic based PIDS and electrified	Guard force patrolling Staff observation

				Door contact and vibration alarms	fence topping on protected area	Local zone alarm management panel
	Assess		A	100% fixed line CCTV of building perimeter 24/7 CCTV monitoring of alarms in SSCR	PTZ cameras scanning fence line	Staff and guard force observation of suspicious activity
	Access Control		A	Supervised ENHANCED 5 EP turnstile for facility access	Supervised ENHANCED 2 EP turnstile on protected area fence.	Regular review of pass access rights
	Insider Threat Measures	Detection of prohibited items	A	100% pat down and metal detection search on store entry X-Ray of bags and equipment on facility entrance	25% search of staff on protected area entry Search dogs present at protected area access points	10% staff search on protected area entry
		Detection of theft	A	100% pat-down and radiation detection searches on store exit	Facility Doorpost radiation detectors	Regular accounting of inventory
		Behavioural aspects	A	Two-person rule for store key access and operations	Monitoring of internal CCTV in SSCR	Access log entry checks for anomalous behaviour.

				Develop Vet and aftercare		
	Response		A	Onsite Armed Response Force	Onsite guard force	Plant personnel
Category III Facility	Delay		B		Building fabric to ENHANCED 5 BF	
	Detect		B		Door contact alarms monitored in SSCR	Local zone alarm management panel Staff reporting suspicious activity
	Assess		B		Patrolling guard sent to investigate alarms CCTV covering access control points	Staff reporting suspicious activity
	Access Control		B		Monitored turnstile to ENHANCED 2 EP	
	Insider Threat Measures		B		10% staff search on entry and exit Regular inventory checks	Search dogs deployed at random intervals
	Response		B		Onsite guard force	Plant personnel