



ONR GUIDE			
CATEGORISATION OF SAFETY FUNCTIONS AND CLASSIFICATION OF STRUCTURES, SYSTEMS AND COMPONENTS			
Document Type:	Nuclear Safety Technical Assessment Guide		
Unique Document ID and Revision No:	NS-TAST-GD-094 Revision 0		
Date Issued:	November 2015	Review Date:	November 2018
Approved by:	D Senior	Programme Director, Regulatory Assurance.	
Record Reference:	TRIM 2015/364369. Folder Number 4.4.1.2535.		
Revision commentary:	Final		

TABLE OF CONTENTS

1. INTRODUCTION	2
2. PURPOSE AND SCOPE	2
3. RELATIONSHIP TO LICENCE CONDITIONS AND RELEVANT LEGISLATION	3
4. RELATIONSHIP TO SAPS, WENRA REFERENCE LEVELS AND IAEA SAFETY STANDARDS ADDRESSED	3
5. ADVICE TO INSPECTORS	4
6. REFERENCES	27
7. GLOSSARY AND ABBREVIATIONS	28
8. ANNEX 1 - EXAMPLES	29
9. ANNEX 2 - FURTHER GUIDANCE ON CLASSIFICATION OF MECHANICAL SYSTEMS	32

1. INTRODUCTION

- 1.1 ONR has established Safety Assessment Principles (SAPs; Ref. 1) to guide its regulatory judgements and actions in the assessment of safety cases for nuclear facilities that may be operated by potential licensees, existing licensees or other dutyholders. The principles presented in the SAPs are supported by a suite of Technical Assessment Guides (TAGs) to further assist ONR's inspectors in their technical assessments supporting regulatory judgements and decisions. This document is one of those TAGs.
- 1.2 A nuclear facility should be designed and operated with layers of defence in depth aimed at preventing faults, ensuring protection in the event that prevention fails and providing mitigation should an accident occur (SAP EKP.3). The identification and categorisation of safety functions and the classification of structures, systems and components (SSCs) are key activities required for the successful, proportionate and balanced implementation of the layers of defence in depth.
- 1.3 Safety function categorisation is the process by which the safety functions, both during normal operation and in the event of a fault or accident, are categorised based on their significance with regard to safety (SAP ECS.1). These safety functions should be identified by following a systematic approach linked to the fault analysis for the facility.
- 1.4 SSC classification is the process by which SSCs are classified on the basis of their significance in delivering the safety functions (SAP ECS.2). The class assigned to an SSC indicates the level of confidence required in its ability to deliver its safety function. It should be used to determine the standards to which SSCs are designed, manufactured, constructed, installed, commissioned, quality assured, maintained, tested and inspected (SAP ECS.3).
- 1.5 Safety function categorisation should be distinct from, and normally be carried out prior to, SSC classification. Safety function category is one of a number of criteria used in choosing and designing the SSC and so should not be influenced by preconceptions as to the ultimate choices and designs that will be made.

2. PURPOSE AND SCOPE

- 2.1 The purpose of this TAG is to provide advice to ONR inspectors on the expectations of the licensee's arrangements for identifying and categorising safety functions and classifying the SSCs that deliver them. Guidance is provided on the factors which ought to be considered in each stage of this process and relevant good practice (RGP) for the categorisation and classification methodology used. ONR inspectors may also use this TAG to assess the licensee's arrangements during the generic design assessment (GDA) or permissioning process for new build or plant modification projects.
- 2.2 This TAG addresses a complex topic with links to a number of different SAPs, a bearing on multiple licence conditions and with interfaces to several other documents. It has been organised to provide the key information early, followed by the supporting detail later. The principles of safety function identification, categorisation and SSC classification are presented first (Sections 5.1 to 5.4). This is followed by some more detailed guidance which sets-out an example of categorisation and classification arrangements to provide an ONR inspector with a starting point from which to judge the adequacy of the licensee's or requesting party's arrangements (Sections 5.5 and 5.6). The final section provides further specific guidance on the way in which SSC class should be reflected across the lifecycle of design, build, operation and decommissioning for a number of disciplines (Section 5.7). Annexes are provided which contain examples to illustrate the categorisation and classification process and provide further supporting material.

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

3. RELATIONSHIP TO LICENCE CONDITIONS AND RELEVANT LEGISLATION

- 3.1 Safety function categorisation and SSC classification affect a number of areas of safety management. However, in particular, nuclear site licence conditions (LC) 14 (safety documentation), 17 (management systems), 23 (operating rules), 24 (operating instructions), 27 (safety mechanisms, devices and circuits) and 28 (examination, inspection, maintenance and testing) are relevant to this guide [Ref. 2].
- 3.2 LC14(1) requires the licensee to make and implement adequate arrangements for the production and assessment of safety cases to justify safety through the lifecycle of the facility. The licensee's arrangements should set-out the methodology for the identification and categorisation of safety functions, the classification of SSCs and how this information should be generated, underpinned and used in the production and assessment of the safety case.
- 3.3 LC17(1) requires that the licensee should establish and implement systems which give due priority to safety. LC17(2) requires the licensee to implement adequate safety management arrangements in respect of all matters which may affect safety. Safety function categorisation and SSC classification are key parts of the means by which these conditions should be met.
- 3.4 LC23(1) requires the licensee to produce an adequate safety case. This should be done in line with the licensee's safety case production arrangements required by LC14. The safety case should therefore identify and categorise the necessary safety functions, identify and classify the SSCs delivering these safety functions and use this in the design and operation of the plant and processes being justified.
- 3.5 LC27 requires the licensee not to operate, inspect, maintain or test its facility unless suitable and sufficient safety mechanisms, devices and circuits (SMDCs) are properly connected and in good working order. They are part of the wider safety measures in place to respond to faults and protect against radiological consequences (see NS-TAST-GD-003 [Ref. 3]). In line with this TAG, their safety functions should be identified and categorised and their SSCs classified.
- 3.6 LC28(1) requires that the licensee makes and implements adequate arrangements for the regular and systematic examination, inspection, maintenance and testing (EIMT) of all plant which may affect safety. This is an important aspect of ensuring that a facility continues to remain capable of delivering the safety functions identified within the safety case with a reliability and level of confidence commensurate with the SSC classifications justified within the safety case.

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

- 4.1 SAPs ECS.1 and ECS.2 [Ref.1] refer directly to safety categorisation and SSC classification respectively. This guide focuses on these principles, although EKP.3-5 and a number of other SAPs are also relevant. Finally, ECS.3 (standards) addresses how SSC classification should be used.
- 4.2 This TAG is closely related to NS-TAST-GD-003 Safety Systems [Ref. 3] which provides specific further detail on the difference between safety-related systems and safety systems, and their design expectations. There are also some similarities with

NS-TAST-GD-035 Limits and Conditions for Nuclear Safety (Operating Rules) [Ref. 4] in relation to the expectations for grading based on safety significance.

- 4.3 The guidance contained in this TAG is derived from BS IEC 61226 Nuclear Power Plants – Instrumentation and Control important to safety – Classification of instrumentation and control functions [Ref. 5]. The scope of that standard deals specifically with the categorisation of safety functions associated with control and instrumentation systems and equipment. The principles adopted in BS IEC 61226 are considered relevant to all nuclear facilities (i.e. not just nuclear power plants) and have been developed within this guidance so that they are applicable to other technical disciplines.
- 4.4 The International Atomic Energy Agency (IAEA) Safety Guide – Safety Classification of Structures, Systems and Components in nuclear power plants [Ref. 6] is applicable to all engineering disciplines and has also been considered during the development of this TAG and the guidance here is consistent with the recommendations made by the IAEA.
- 4.5 Western European Nuclear Regulators Association (WENRA) safety reference levels for existing reactors Issue G: Safety Classification of SSCs Safety: Design has been considered during the development of this TAG. The Issue G objective states that all SSC important to safety shall be identified and classified on the basis of their importance for safety. [Ref. 7].

5. ADVICE TO INSPECTORS

5.1 SAFETY FUNCTIONS AND CATEGORISATION

5.1.1 DEFINITION AND PURPOSE OF SAFETY FUNCTIONS

- 5.1.1.1 A safety function is a specific purpose or objective that must be accomplished in the interests of safety [Ref. 5]. It should usually be specified or described with minimal or no reference to the physical means of achieving it. This provides some conceptual separation of a safety 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 and modifications.
- 5.1.1.2 Safety functions are used to define the safety purposes and objectives required within a nuclear facility during both normal operation as well as following any fault or accident condition which may arise. Safety functions should be applied, as appropriate, to all five levels of the hierarchy of defence in depth (SAP EKP.3 [Ref. 1]).

Engineering principles: key principles	Defence in depth	EKP.3
Nuclear facilities should be designed and operated so that defence in depth against potentially significant faults or failures is achieved by the provision of multiple independent barriers to fault progression.		

- 5.1.1.3 Those safety functions that are needed during the normal operation of a facility usually relate to levels 1-2 of the hierarchy. They describe the safety functions that are delivered by the safety-related systems and operator actions that enable the facility to undertake its normal duties. Such functions are centred on either preventing failures by design, or, where failures occur, ensuring that abnormal occurrences are detected and controlled to avoid the plant departing from the normal operating envelope [Ref. 3].
- 5.1.1.4 Those safety functions that are needed in response to a fault or accident condition usually relate to levels 3-5 of the hierarchy. They describe the safety functions that are

delivered by the safety systems in place to control faults and protect from escalation beyond the design basis or, if an accident situation arises, to mitigate against further escalation and radioactive release.

5.1.1.5 ONR inspectors should be aware that safety functions are referred to by some licensees as safety functional requirements (SFR). In some cases, they may be given a level or other descriptor related to their position within a hierarchical functional breakdown (see Section 5.1.2). For example, a “level 1” or “demand” function for a high level goal, or a “level 3” or “system” function for a more specific requirement that will be aligned to a specific system within a facility. Separately, safety functions or SFRs may also be qualified to distinguish the type or origin of a safety function or its level within the hierarchy of defence in depth. For example, those relating to normal operation may be prefixed as “duty” functions to distinguish them from “fault” functions and/or “accident” functions.

5.1.2 IDENTIFICATION OF SAFETY FUNCTIONS

5.1.2.1 The fundamental safety functions are the highest level objectives that must be delivered during both normal operation and under fault conditions. Under accident conditions, the circumstances are likely to be such that control of one or more functions has been lost; however, the same fundamental objectives remain and the focus should be on restoring control.

5.1.2.2 The fundamental safety functions for a nuclear reactor (see paragraph 540 of the SAPs and SAP ERC.1) [Ref. 1], are the:

- control of reactivity (including preventing re-criticality following an event);
- removal of heat from the core;
- confinement of radioactive material.

Engineering principles: reactor core	Design and operation of reactors	ERC.1
The design and operation of the reactor should ensure the fundamental safety functions are delivered with an appropriate degree of confidence for permitted operating modes of the reactor.		

5.1.2.3 For non-reactor facilities (see paragraph 159 of the SAPs and SAP EPE.1 [Ref.1]), analogous fundamental safety functions can be derived based on the hazards which are present and the controls which are needed. The control of reactivity and the prevention of inadvertent criticality can apply more widely to any process that handles fissile material. The control of temperature applies more widely to processes involving heat-generating radioactive material or exothermic chemical reactions. The confinement of radioactive material always applies and in some cases, it may be appropriate to differentiate the control of direct radiation exposure as a fourth function.

Engineering principles: chemical engineering	Design and operation	EPE.1
The design and operation of nuclear chemical processes and facilities should be fault tolerant and ensure safety functions are delivered with suitable capability and sufficient reliability and robustness.		

5.1.2.4 The fundamental safety functions can be decomposed into more specific sub-functions through a top-down breakdown of the fundamental requirements. For example:

- the on-going normal control of temperature in a spent fuel pond may identify the requirements for temperature and level monitoring, leak detection, coolant circulation and the control of heat transfer to a heat sink;
- the restoration of reactivity control following a specific fault in a chemical processing plant may identify the requirements for the detection of an unsafe condition and storage and injection of a reactivity poison;
- the confinement of radioactive material following a reactor accident may identify the need to avoid the formation of an explosive atmosphere to prevent a detonation challenging the integrity of a containment building.

5.1.2.5 This top-down safety function breakdown, applied to both normal operations and during fault or accident conditions, provides a method for achieving the structured identification of safety functions in line with SAP EKP.4 [Ref.1] although there are other ways in which the licensee could choose to achieve this.

Engineering principles: key principles	Safety function	EKP.4
The safety function(s) to be delivered within the facility should be identified by a structured analysis.		

5.1.2.6 It should be noted that numerous discipline-specific standards and sources of RGP exist to define the processes that should be adopted throughout the lifecycle of a facility. In addition, WENRA reference levels [Ref. 7] state that the design shall take into account the effects of operational conditions over the lifetime of the plant and, when required, the effects of accident conditions on their characteristics and performance.

5.1.2.7 The safety function breakdown should usually continue to at least the point at which the safety functions become clearly attributable to the engineered systems that will be subject to SSC classification. This is discussed further in section 5.3 and explored in the examples in Annex 1.

5.1.3 SAFETY FUNCTION CATEGORISATION

5.1.3.1 SAP ECS.1 [Ref. 1] outlines the main expectations of safety functions categorisation.

Engineering principles: safety classification and standards	Safety categorisation	ECS.1
The safety functions to be delivered within the facility, both during normal operation and in the event of a fault or accident, should be identified and then categorised based on their significance with regard to safety.		

5.1.3.2 It is an expectation of the SAPs (see paragraph 160 and SAP FA.9) that the licensee's categorisation scheme should be linked explicitly with the design basis analysis (DBA).

5.1.3.3 The licensee's categorisation scheme should:

- define the safety function categories and the process through which safety functions are categorised;
- provide details on how any factors influencing the categorisation should be sourced and used (e.g. it may state that initiating fault frequencies should be drawn from the probabilistic safety analysis (PSA));

- employ an appropriate number of safety function categories (three categories are recommended by IAEA guidance [Ref. 6]);
- be distinct from SSC classification to avoid confusion;
- be specific enough to enable different users to consistently assign the same categorisation to a safety function;
- include appropriate flexibility to take account of unforeseen circumstances.

5.1.3.4 In line with paragraph 161 of the SAPs [Ref. 1], the category assigned to a safety function should take into account:

- the consequence of failing to deliver the safety function;
- the likelihood that the function will be called upon; and
- the extent to which the function is required, either directly or indirectly, to prevent, protect against or mitigate the consequences of initiating faults.

5.1.3.5 As noted in Section 5.1.1, the safety functions should be described separately to the engineering means by which they will be delivered. Safety function categorisation therefore should not usually take account of redundancy, diversity or independence within the SSC delivering the function. For example, if the safety function was the relief of over-pressure, then its categorisation should not be altered by the design of the pressure relief system itself. Similarly, the category of a safety function for the removal of decay heat from a reactor should not be affected by the number or nature of the heat transfer systems in place to achieve it.

5.1.3.6 An example categorisation scheme is given in Section 5.5.

5.2 STRUCTURES, SYSTEMS AND COMPONENTS AND THEIR CLASSIFICATION

5.2.1 TERMINOLOGY – SAFETY SYSTEMS AND SAFETY-RELATED SYSTEMS

5.2.1.1 The SAPs describe an SSC as an item important to safety that provides a safety function. There are two distinct groups of SSCs:

- some SSCs enable the facility to undertake its normal operational duties (whether or not they also play a role in responding to a fault or accident);
- other SSCs have no role in normal operations and are exclusively present only to respond to a fault or accident.

5.2.1.2 In understanding this difference, the concept of the unprotected plant is helpful [Ref. 3]. The unprotected plant is made up from those SSCs that are essential to enable the facility to undertake normal operations. Some of these SSCs may also have roles in the response to fault or accident conditions alongside safety systems. These SSCs make up what are known as safety-related systems and include:

- the reactor pressure vessel (RPV), heat transfer systems and other items needed to generate electricity at a power station;
- the vessels, valves and other items needed for the day-to-day storage, production and other duties in a nuclear manufacturing or chemical plant.

These safety-related SSCs should be classified according to the nuclear safety significance of their contribution to safety functions that they support. As noted above, this can include safety functions associated with normal operation and safety functions associated with the response to a fault or accident.

5.2.1.3 Some SSCs are not part of the unprotected plant but are provided exclusively to respond to a faults or accidents. They act to protect against a radiological consequence and are known as safety systems. Examples include:

- the main guard lines, diverse shut down systems, over-pressure protection equipment, emergency cooling systems and other items at a power station;
- the gamma monitors, fire protection, sump level detectors, flammable gas detectors and other items in a nuclear manufacturing or chemical plant.

These SSCs are part of the safety systems and other features that implement the safety functions associated with the response to faults or accidents. They should be classified according to the nuclear safety significance of their contribution to achieving these safety functions.

5.2.1.4 The complete protected plant is the combination of the unprotected plant together with those additional SSCs provided to respond to faults or accidents. The safety functions associated with the SSCs should be clearly identified within the safety case. This is a part of SAP EKP.5 [Ref. 1] which is discussed further in Section 5.2.2 below.

Engineering principles: key principles	Safety function	EKP.5
Safety measures should be identified to deliver the required safety function(s).		

5.2.2 SAFETY MEASURES AND HUMAN FACTORS

5.2.2.1 SAP ECS.2 [Ref. 1] focuses on the application of classification to SSCs; however, paragraph 164 of the SAPs states that where safety functions are delivered or supported by human action, these human actions should be identified and classified. It notes that the methods for classification should be analogous to those used for classifying SSCs. This view is supported by SAP EHF.3 [Ref. 1], which states the expectation that a systematic approach to the identification of human actions that can impact safety is needed for both normal operations as well as during fault or accident conditions. SAP EHF.4 [Ref. 1] states that any administrative controls needed in support of such actions should also be identified. NS-TAST-GD-063 [Ref. 8] contains more guidance in this area.

Engineering principles: human factor	Identification of actions impacting safety	EHF.3
A systematic approach should be taken to identify human actions that can impact safety for all permitted operating modes and all fault and accident conditions identified in the safety case, including severe accidents.		

Engineering principles: human factor	Identification of administrative controls	EHF.4
Administrative controls needed to keep the facility within its operating rules for normal operation or return the facility back to normal operations should be systematically identified.		

5.2.2.2 Although this TAG focuses on the classification of SSCs, it is expected that the licensee will also identify and classify any human actions using an equivalent methodology. This may be through the provision of separate but analogous arrangements for SSC and human actions, or, the licensee may implement a combined approach that classifies complete safety measures.

5.2.2.3 The term safety measure is used to encompass both the human actions and SSCs needed in the delivery of safety functions. A safety measure is defined as a safety system, or a combination of procedures, operator actions and safety systems that protects against a radiological consequence, or a specific feature of plant designed to prevent or mitigate a radiological consequence by passive means. SAP EKP.5 [Ref. 1] states that safety measures should be identified against the delivery of the safety functions at all levels of the defence in depth.

5.2.3 SSC CLASSIFICATION

5.2.3.1 SAP ECS.2 [Ref. 1] outlines the main expectations of SSC classification.

Engineering principles: safety classification and standards	Safety classification of structures, systems and components	ECS.2
Structures, systems and components that have to deliver safety functions should be identified and classified on the basis of those functions and their significance to safety.		

5.2.3.2 The licensee's classification scheme should:

- define the classes of SSCs and the process for determining the way in which they are assigned;
- be used for nuclear safety purposes and not used in the context of the control of any non-safety aspects (e.g. production capability or financial value);
- detail how any factors influencing the SSC class should be sourced and used;
- employ an appropriate number of SSC classes (three categories are recommended by IAEA guidance [Ref. 6]);
- be distinct from safety function categorisation to avoid confusion;
- be specific enough to enable different users to consistently assign the same classification to an SSC;
- include appropriate flexibility to take account of unforeseen circumstances.

5.2.3.3 In line with paragraph 165 of the SAPs [Ref. 1], the class assigned to an SSC should take into account:

- the category of safety function(s) to be performed by the item;
- the probability that the item will be called upon to perform a safety function;
- the potential for a failure to initiate a fault or exacerbate the consequences of an existing fault, including situations where the failure affects the performance of another SSC; and
- the time following any initiating fault at which, or the period throughout which, it will be called upon to operate in order to bring the facility to a stable, safe state.

5.2.3.4 Once an SSC has been classified, the usual presumption ought to be that all sub-components of the SSC inherit that overall classification. If it is necessary to assign a lower classification to some sub-components, then this should normally be supported either by further refinement of the safety functions and their categorisation, or, for simple cases, by an argument explaining the role (or not) of the sub-component in the delivery of the safety function. This may take account of the redundancy, diversity or independence within the overall system design. Section 5.3 and examples in Annex 1 provide further guidance.

5.2.3.5 The detailed approach to SSC classification may depend on the specialist discipline area. For example, the classification process for control and instrumentation systems in nuclear power plants is carried out according to BS IEC 61226 [Ref. 5]. Discipline-specific guidance is provided in Section 5.7.

5.2.4 SSC RELIABILITY

5.2.4.1 The class of an SSC is fundamentally linked with its reliability (this is discussed further in Ref. 3). Using the three-class scheme recommended by the SAPs (expanded on later in this TAG), Table 1 shows the link between the class of the system and the failure frequency (ff) for continuously-operating systems and the probability of failure-on-demand (pfd) for demand-based systems.

5.2.4.2 For normal operation systems that are run intermittently the failure frequencies would normally be expected to be calculated assuming continuous operation.

SSC Class	Failure frequency / year (ff)	Probability of failure on demand (pfd)
Class 1	$10^{-3} \geq ff \geq 10^{-5}$	$10^{-3} \geq pfd \geq 10^{-5}$
Class 2	$10^{-2} \geq ff > 10^{-3}$	$10^{-2} \geq pfd > 10^{-3}$
Class 3	$10^{-1} \geq ff > 10^{-2}$	$10^{-1} \geq pfd > 10^{-2}$

Table 1 Relationship between SSC class and the failure frequency and probability of failure on demand [Ref. 3].

5.2.5 USES OF SSC CLASSIFICATION

5.2.5.1 The intent of SAP ECS.3 and its supporting paragraphs [Ref. 1] is that the range of lifecycle activities associated with an SSC are controlled by codes and standards appropriate to its class. This is reinforced in various other SAPs and their supporting guidance in Ref. 1.

5.2.5.2 As SSC class is directly connected to reliability (see Section 5.2.4 above), it is therefore 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 SSC into service (such as the category of an LC 22 submission (see NS-INSP-GD-022 [Ref. 9])).

Engineering principles: safety classification and standards	Standards	ECS.3
Structures, systems and components that are important to safety should be designed, manufactured, constructed, installed, commissioned, quality assured, maintained, tested and inspected to the appropriate codes and standards.		

5.3 THE LEVEL TO APPLY CATEGORISATION AND CLASSIFICATION

5.3.1 Safety functions can be broken-down into an increasingly detailed set of subsidiary functions and categorisation of these functions can be carried out at a variety of levels. Likewise, the SSCs that make up the plant systems can be decomposed into an increasingly more detailed array of sub-systems and components. Similarly classification can be applied at a number of levels within this hierarchy. There is often a close relationship between the functional breakdown and the systemic breakdown but there may not be a one-to-one mapping between them.

5.3.2 The licensee's arrangements should define the approach to any functional or systemic breakdown and the point at which categorisation and classification are undertaken. This section provides guidance on the expectations of these arrangements. Some supporting examples are provided in Annex 1.

- 5.3.3 The process of safety function breakdown should continue to at least the point at which the roles of the different safety systems and safety-related systems in the delivery of these functions become clear. Safety function categorisation should be applied at no higher than this level to avoid over-simplification and possible mis-categorisation. In some cases, a further breakdown may be needed for a more detailed understanding of the detailed functions and their categories.
- 5.3.4 The corresponding classification of SSCs, either individually or as part of a group of SSCs making up a safety system or safety-related system, should be carried out at the level of detail at which the safety functions have been categorised.
- 5.3.5 When classifying a group of SSCs as a safety system or safety-related system, the group should generally extend to the combination of equipment needed to deliver a particular safety function in a particular way (also see Section 4.1 of Ref. 3). This usually means those individual SSCs that are physically connected together (whether that be mechanically, electrically, hydraulically or pneumatically). It includes all elements of instrumentation, processing and actuation, together with any required support services such as cooling, lubrication or power supply, and any redundant channels, trains or divisions.
- 5.3.6 Separate and physically unconnected systems, whether they deliver a different safety function or serve to provide a diverse means of implementing the same function, should usually be classified separately. Where two or more systems work closely together, are co-located or share other similarities such that they are vulnerable to common-cause events, then it may be appropriate to extend the classified combination to include them all together. However, including preventative, protective and/or mitigative elements within a single classified combination should be avoided:
- a safety-related normal operational system with a preventative function (levels 1 and 2 of the hierarchy of defence in depth) should not be included and classified as part of a single larger "system" alongside safety systems delivering a protective function in response to a fault (level 3);
 - mitigating safety systems (levels 4 and 5) should not be included and classified alongside protective safety systems (level 3) as part of an overall "system" which is classified as a single item.
- 5.3.7 The intent of the above guidance is to limit the inadvertent dilution of the integrity of preventative measures through the presence of protective measures and likewise for protective versus mitigative means. This reinforces the defence in depth principle that the levels are independent and that earlier barriers do not take credit for later ones. Some SSCs may have roles that span across the hierarchy; however, wherever possible, these should be identified through distinct safety functions to understand the differences between their preventative, protective and/or mitigative functions and treat them appropriately.

5.4 FACILITY LIFECYCLE

- 5.4.1 The provision of properly defined safety functions and SSCs are fundamental for the development of robust safety cases and well-engineered protective measures for all of the possible states in the lifecycle of a facility. This includes:
- normal operational states including power generation, usual production, standby states, shutdown states, outage or maintenance states;
 - other lifecycle states including construction, commissioning, post-operational clean-out, decommissioning;
 - operational abnormalities or fault states within the design basis;
 - states which may have arisen because of a beyond design basis event, malicious act or the escalation of a design basis fault;

- situations in which significant relocations or releases of radioactive material have occurred and need to be managed.

5.4.2 The role of many safety functions and SSCs may be described within the lifecycle V-diagram of a facility and are illustrated in Figure 1. The following descriptions of each of the phases of the lifecycle are intended to provide a rough guide. More information is contained in BS IEC 61513 [Ref. 10].

- **Project definition.** The functional requirements for a facility are initially produced during the conceptual design stage and developed through iterations as the design matures. The safety functions are identified.
- **Categorisation.** A structured analysis should be used to determine the safety functions needed during normal operation and during fault or accident conditions. Safety functional requirements should include, for example, system architecture, system sizing (flow rates, pressures, heat loads, response times, etc.), seismic withstand capability. These functions should be categorised on the basis of their importance to nuclear safety. See Section 5.1.
- **Classification.** The SSCs making up the safety-related systems and safety systems of the facility should be classified on the basis of their importance to nuclear safety. See Section 5.2.
- **Design and realise protected plant.** The SSCs are designed, produced, manufactured, fabricated and tested to ensure they satisfy the requirements specifications. Assurance systems will be used to provide confidence that individual components of the system operate as expected.
- **Implement SSCs.** The SSCs are installed, commissioned and verified to standards appropriate to their classification. See Sections 5.2 and 5.7.
- **Implement safety functions.** The overall safety performance of the plant should be validated by showing that the realised design delivers the safety functions to their acceptance requirements. See Section 5.1.
- **Operations.** During the development phase, criteria for the safe operation and EIMT will have been developed in order that their safety performance is maintained. Modification and experiments undertaken on a facility should be graded using a process cognisant of the safety category of any relevant safety functions and the safety classification for any applicable SSCs.
- **Decommissioning.** During the development stage thought should be given to the functions that will be required for, or relevant to, the future decommissioning of the facility.

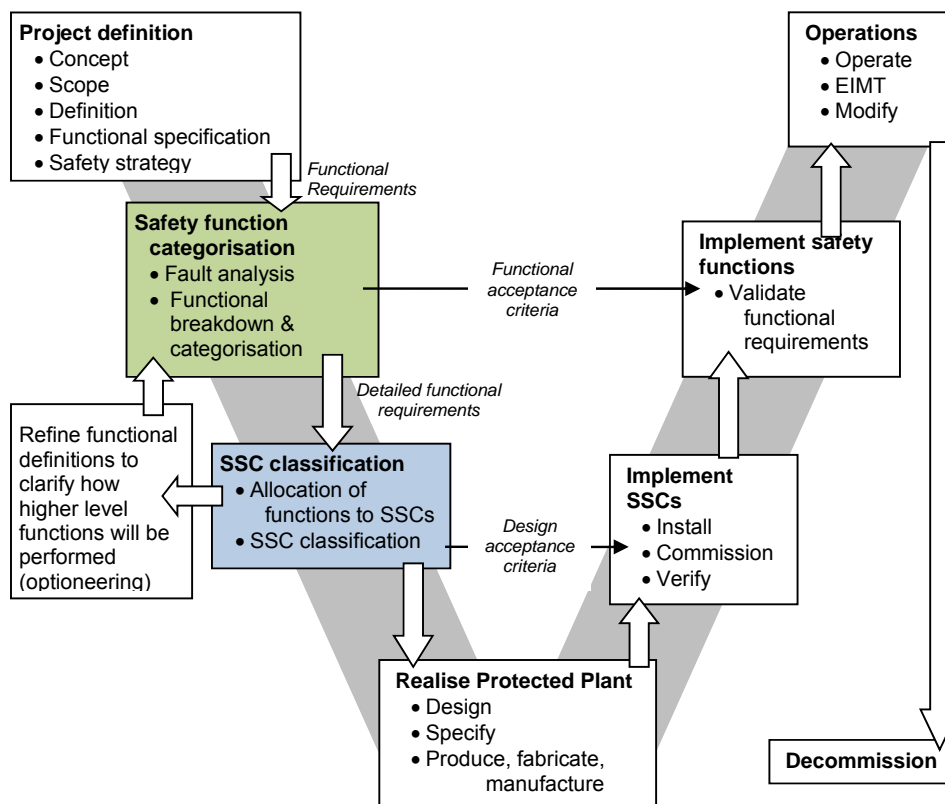


Figure 1 – Role of safety function categorisation (green box) and SSC classification (blue box) within the lifecycle model (“V-diagram”)

5.5 EXAMPLE SAFETY FUNCTION CATEGORISATION SCHEME

5.5.1 APPROACH

5.5.1.1 Section 5.1.3 has already set out the overarching expectations of a safety function categorisation scheme. The licensee should choose a suitable scheme in the context of aspects such as:

- the nature of its operations (e.g. generation compared to reprocessing);
- the safety case structure (e.g. a building-orientated safety case compared to a process-orientated safety case);
- any interfaces in safety arrangements (e.g. an interface with a submarine safety justification or a neighbouring licensed site with which some safety-related services may be shared).

5.5.1.2 This section sets out **the outline** of a process that would meet the expectations of ECS.1 and Section 5.1. ONR inspectors should view it **as a starting point** to inform their assessment of the suitability and sufficiency of the core of the licensee’s arrangements. **It is not a prescribed method and other approaches can be used.**

5.5.1.3 The suggested scheme makes use of the three categories recommended in the SAPs paragraph 160 [Ref. 1]:

- Category A – any function that plays a principal role in ensuring nuclear safety;
- Category B – any function that makes a significant contribution to nuclear safety;
- Category C – any other safety function contributing to nuclear safety.

5.5.1.4 Figure 2 shows a diagram that draws and expands upon the categorisation factors listed under ECS.1. The approach given is a two-step process:

- Step 1 – an initial categorisation, based on quantified values for the initiating event frequencies and the consequences of failure. This is intended to meet the expectation that deterministic analysis is used as the primary influence in categorisation;
- Step 2 – a refinement step which considers more qualitative factors.

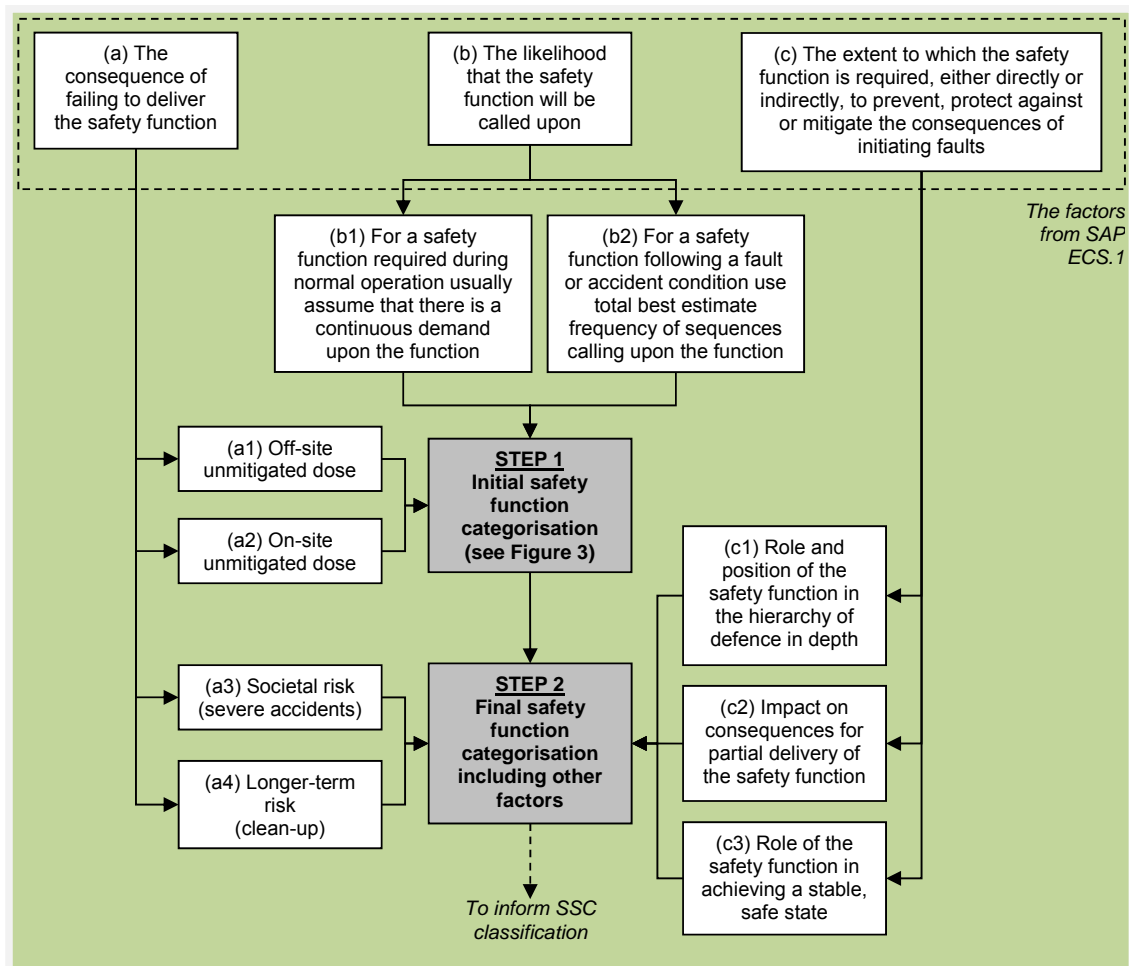


Figure 2 – safety function categorisation scheme

5.5.2 STEP 1 – INITIAL CATEGORISATION

5.5.2.1 The first step involves the assignment of an initial expectation of a safety function category using a process driven mainly by the DBA. The two most important factors in this determination, in accordance with IAEA guidance [Ref. 6], are: (a) the consequences should the safety function not be performed; and (b) the likelihood with which a demand is placed upon the safety function.

5.5.2.2 The consequence (a) of failing to deliver the safety function is interpreted in terms of the potential unmitigated radiological doses that could be received by a person on the licensed site and a person outside the licensed site. For safety functions associated with design basis faults (as per SAP Target 4 [Ref. 1]), the consequences of failing to perform the function should already have been calculated on a conservative basis. For safety functions not addressed within DBA, a best-estimate approach is acceptable.

This means that additional dose calculations rarely need to be undertaken as the appropriate values can be drawn from the existing fault analysis.

- 5.5.2.3 The likelihood (b) of being called upon is interpreted as the demand frequency of the safety function. For a normal operation safety function associated with a safety-related system, the demand should usually be assumed to be continuous (b1). For a safety function associated with a safety system, the demand should be calculated as the total best estimate frequency of fault sequences upon which the safety function will be required (b2).
- 5.5.2.4 Figure 3 shows the regions of frequency and consequence space in which the initial categorisation of a safety function may be assigned. There are two diagrams to consider here – one for the dose off-site (a1 and Figure 3a) and one for the dose on-site (a2 and Figure 3b). The highest category resulting from the use of both diagrams should be used. Safety functions lying close to boundaries between categories should be considered carefully and, where there is uncertainty, assumed to lie within the more demanding category.
- 5.5.2.5 For reference, the basic safety objective (BSO) and the basic safety level (BSL) from SAP Target 4 [Ref. 1] are included.
- 5.5.2.6 Should the licensee follow an approach similar to the diagram in Figure 3, they should select their own categorisation regions to reflect the context of their operations, safety case and interfacing arrangements. The demarcation in Figure 3 is intended to serve as **a starting point** for assessing the adequacy of categorisation regions if used within the licensee's arrangements.

5.5.3 STEP 2 – REFINEMENT

- 5.5.3.1 The second step incorporates a number of more qualitative factors. Detailed guidance is not provided here; instead, the factors identified should be seen as triggers for further understanding of the licensee's own arrangements in the context of the nature of the facility in question and the specific safety function being categorised.
- 5.5.3.2 The qualitative factors suggested include the consideration of (a3) societal risk (for severe accidents – also see SAP Target 9 [Ref. 1]) and (a4) the safety considerations (longer term risks) associated with accident recovery and remediation. Both of these aspects may necessitate an increase in the initial safety function categorisation.
- 5.5.3.3 This step also considers (c1) the role and position of the safety function in the hierarchy of defence in depth. It may be appropriate, for example, to lower the category of a preventative safety function if the category associated with an alternative protective function is increased to compensate. Depending on how the safety functions have been constructed, this is one approach to resolving the difficulties associated with providing very high integrity normal operation systems. This is discussed further in Section 5.6.4.
- 5.5.3.4 Another factor is (c2) the potential reduction or exacerbation in consequences should there only be partial delivery of the safety function.
- 5.5.3.5 The last factor (c3) relates to the significance of the safety function in achieving a stable, safe state. This is defined by the SAPs as the state of the facility once stabilisation of any transient or fault has been achieved i.e. the facility is subcritical, adequate heat removal is ensured and continuing radioactive releases are limited. It also provides the flexibility to include for any broader considerations about where the safety function sits within the hierarchy of defence in depth. A function that extended over more than one level of the hierarchy, for example, may warrant an increase in its categorisation.

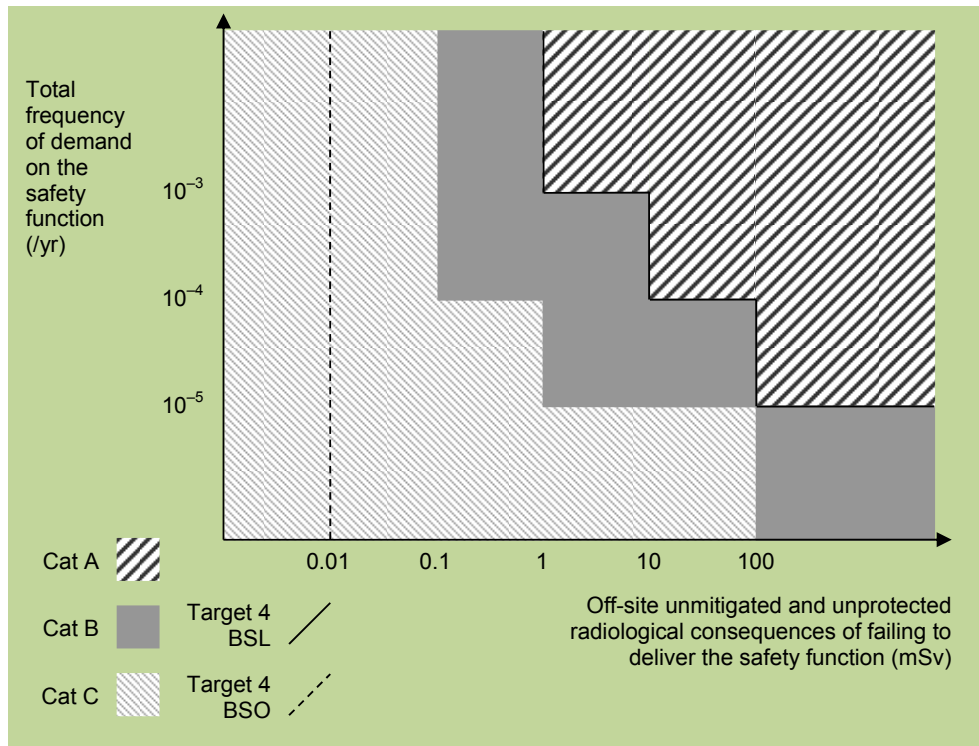


Figure 3a – Off-site frequency/consequence regions for initial safety function categorisation (see Section 5.5.2)

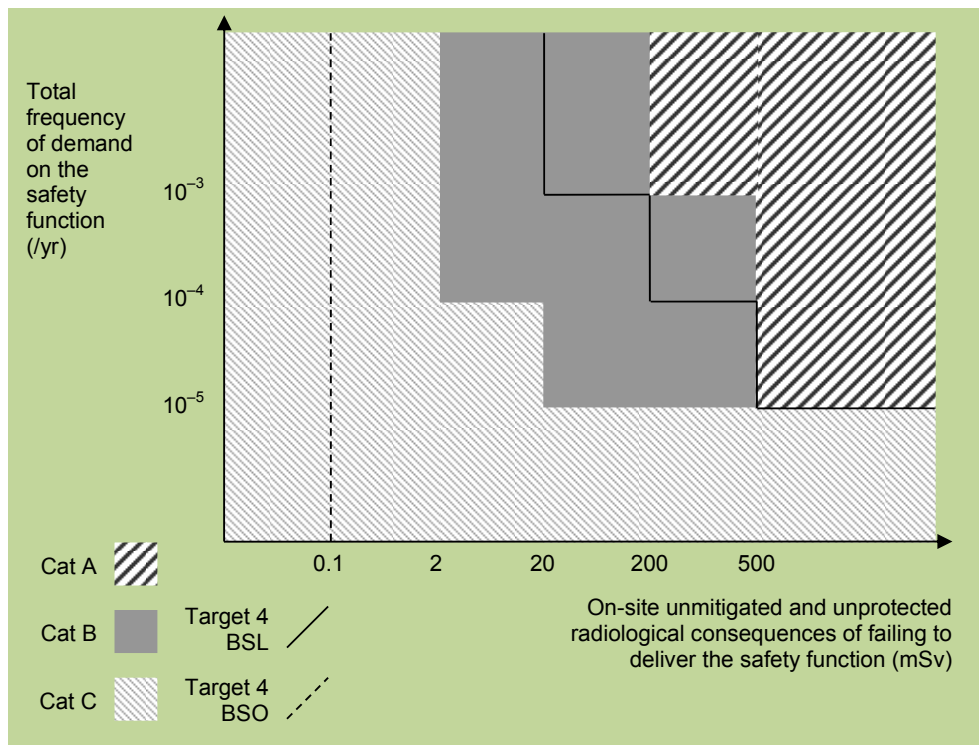


Figure 3b – On-site frequency/consequence regions for initial safety function categorisation (see Section 5.5.2)

5.6 EXAMPLE SSC CLASSIFICATION SCHEME

5.6.1 APPROACH

5.6.1.1 This section sets out **the outline** of an SSC classification scheme that would meet the expectations of ECS.2 [Ref. 1] and Section 5.2.3. As with the example categorisation process this guidance should be used by ONR inspectors **as a starting point** when assessing the licensee's arrangements.

5.6.1.2 It makes use of the three-class scheme recommended in the SAPs paragraph 166 [Ref. 1]:

- Class 1 – any SSC that forms a principal means of fulfilling Category A safety function;
- Class 2 – any SSC that makes a significant contribution to fulfilling a Category A safety function, or forms a principal means of ensuring a Category B safety function;
- Class 3 – any other SSC contributing to a categorised safety function.

5.6.1.3 Figure 4 shows a diagram of the suggested classification scheme that draws and expands upon the classification factors listed in ECS.2 [Ref. 1]. As with categorisation, it is a two-step process with an initial classification assignment followed by a refinement step that considers further aspects.

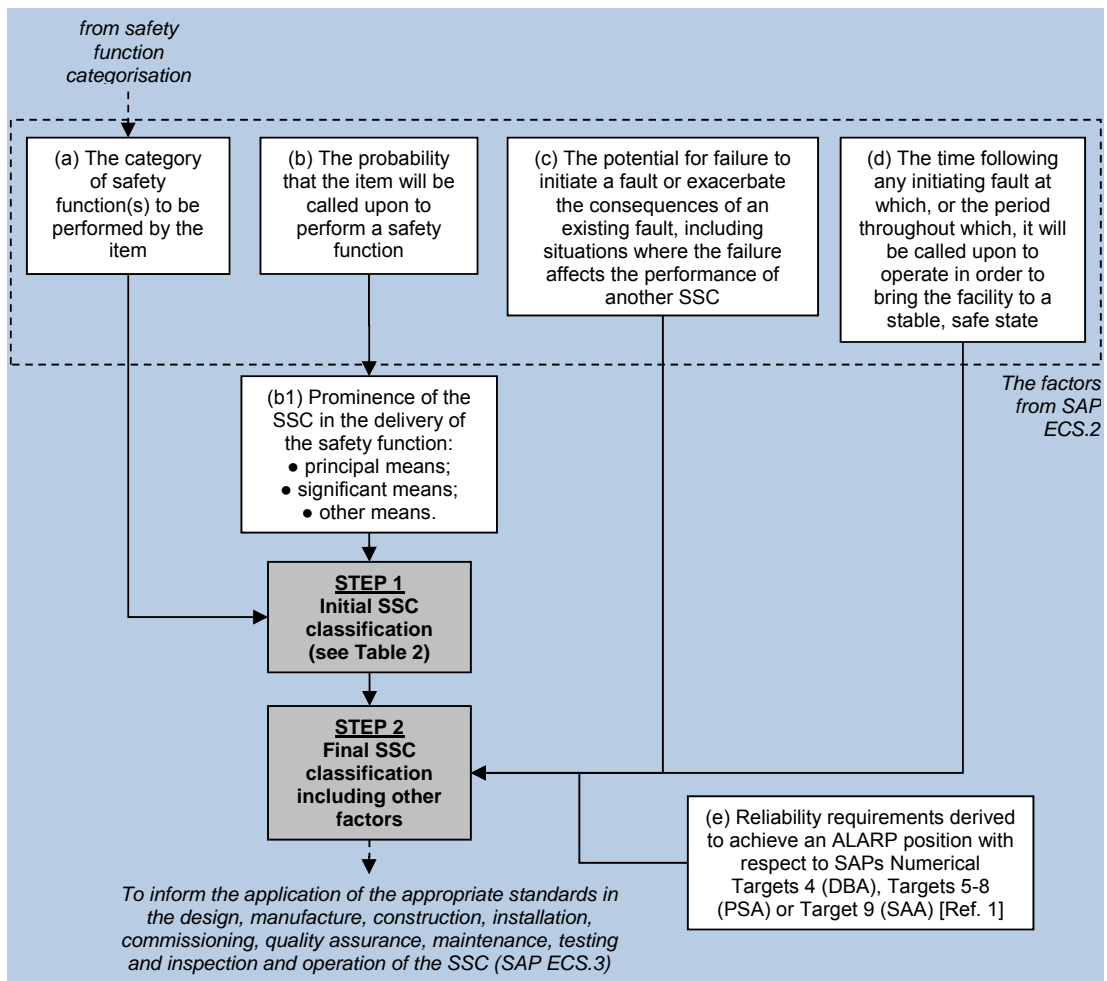


Figure 4 – SSC classification scheme

5.6.2 STEP 1 – INITIAL CLASSIFICATION

5.6.2.1 The first step involves the assignment of an initial expectation of the SSC classification using Table 2 below. The key factors in this assignment are (a) categorisation of a safety function(s) to be performed by the item together with (b) the probability that the item will be called upon to do them. This is interpreted as the prominence of the SSC in the delivery of the safety function:

- For SSCs delivering preventative functions as part of the normal operation of the plant then it is likely that these will be in continuous or frequent demand. They should initially be considered as a principal means of delivering the safety function, however, see Section 5.6.4 below on prevention versus protection;
- For SSCs delivering protective or mitigative functions in response to a fault or accident condition, then the principal/significant/other means normally relates to the position in the hierarchy of defence in depth and the order in which the SSCs respond to the progression of a fault, i.e. first/second/third.

5.6.2.2 The main expectation is that the principal/first line means of providing a safety function takes its classification based directly from the category of safety function: Class 1 for Category A, Class 2 for Category B and Class 3 for Category C. Should they be necessary (Section 4.2 of Ref. 3), any SSCs assigned to a backup measure may then step-down to the next lower class in line with the table. If two means of providing a safety function are identified then one of them should be identified as the principal means. It is not normally appropriate to identify both systems merely as significant means, as this may evade the higher classification associated with the principal means of delivering the particular category of safety function.

		Prominence of the SSC in the delivery of the safety function		
		Principal means	Significant means	Other means
Safety function	Category A	Class 1	Class 2	Class 3
	Category B	Class 2	Class 3	
	Category C	Class 3		

Table 2 – Initial SSC classification.

5.6.2.3 As a single SSC may contribute to the delivery of a number of safety functions, its class should be determined by the highest category function that it is intended to deliver.

5.6.2.4 It is ONR's expectation that the combinations of categorisation and classification presented in Table 2 above would be achieved for new plant and would represent the modern standard for the assessment of existing plant in any periodic review of safety or for modifications. A robust justification would be needed to demonstrate otherwise. Given a strong Class 1 principal means, for example, it may be acceptable in some circumstances to support Class 3 significant means in the delivery of a Category A function. This of course would be subject to an adequate justification of ALARP and the other factors listed under step 2 of the classification process below.

5.6.2.5 Typically, ONR expects that Class 1 and Class 2 SSCs will feature within the safety measures identified in DBA. This is because DBA should be applied to faults with unmitigated consequences exceeding the Target 4 BSL and the safety functions associated with these faults would normally be expected to be Category A or

Category B (noting Figures 3a and 3b). These functions would usually be delivered by Class 1 and Class 2 SSC (noting Table 2); however, some Class 3 SSCs may also be identified within DBA should they be provided in support of these functions (other means of Category A or significant means of Category B).

5.6.3 COMBINING SYSTEMS AND SAFETY CLASSES

- 5.6.3.1 As discussed in Section 5.3, the safety functions should usually be broken-down to the point at which they become clearly attributable to a group of SSCs making up a safety system or safety-related system. Such groups can be classified as a single item, with the individual SSCs inheriting the safety class of the whole system. In some situations it may be better to decompose the safety functions further and assign different classes to individual SSCs depending on their role in the delivering these more specific functions.
- 5.6.3.2 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 (also see Ref. 3). Where this is unavoidable (e.g. where alternative reasonably practicable means of achieving the required functionality and / or safety performance are not readily available), in line with the guidance in Section 5.3, the recommended approach would be to consider the multiple lower class systems as a whole and demonstrate that the combination achieves the integrity of the original higher class system that was being replaced.
- 5.6.3.3 Considering separate systems as a single classified combination may be preferable when there are similarities in location or function such that they are vulnerable to common-causes. However, to reiterate the guidance in Section 5.3, combining preventative, protective and mitigative elements in a single classified combination should be normally be avoided. For example, the replacement of a Class 1 protection system with a Class 2 protection system plus a Class 3 mitigative system would require robust justification, as this has diminished the integrity of level 3 (protection) of the hierarchy of defence in depth by replacing it with some mitigation at level 4.

5.6.4 PREVENTION VERSUS PROTECTION

- 5.6.4.1 In line with the approach to defence in depth, the focus should be on preventing a fault occurring and thereby limiting the demand placed on protection systems: the integrity of the systems delivering preventative safety functions should not therefore be automatically lowered simply because a safety system delivering a protective function exists. This is reinforced by the scheme in Figure 4, which will usually encourage a high class for a preventative system as a principal/first line means of delivering a safety function.
- 5.6.4.2 However, in many cases, it is not practicable for the normal operation system to carry a high safety class and it is appropriate for this to be reduced in favour of increasing the class of a protective safety system. Normal plant control systems often feature in these circumstances, although they are not alone. This is acceptable but a justification of the reduced focus on the preventative defence in barriers should be provided.
- 5.6.4.3 There are a number of ways in which the licensee's arrangements may practically deal with this topic and ONR does not prescribe a solution. One method would be to distinguish preventative and protective functions and amend their categorisation (see Section 5.3). An alternative may be to provide further guidance on how "principal", "significant" and "other" can be interpreted when classifying an SSC.

5.6.5 NUMBER AND QUALITY OF SAFETY SYSTEMS

5.6.5.1 There are no fixed requirements as to the number of safety systems required to deliver a safety function. A single Class 1 safety system, for example, might be suitable and sufficient in providing a Category A safety function in some circumstances; on the other hand, a Class 1 safety system backed-up by a Class 2 system may be required, particularly for frequent faults.

5.6.5.2 As also noted in Section 5.6.6 below, the assessment of whether the number and quality of safety systems is appropriate goes beyond the application of categorisation and classification and is addressed by other guidance such as Ref. 3. Specific SAPs may be relevant to certain aspects, such as ERC.2 and EDR.4 [Ref. 1].

5.6.5.3 SAP ERC.2 [Ref. 1] expects that at least two diverse systems should be provided to ensure that a civil reactor can be shutdown and maintained sub-critical. If reactor shutdown is identified as a safety function, then this SAP will usually drive a need for two systems to deliver it. An alternative approach could be develop two different safety functions against this overriding requirement and then identify a system against each one.

Engineering principles: reactor core	Shutdown systems	ERC.2
At least two diverse systems should be provided for shutting down a civil reactor.		

5.6.5.4 The single failure criterion, expressed in SAP EDR.4 [Ref.1], is a specific expectation that, in all but exceptional circumstances, applies to any system that is the principal means of delivering a Category A safety function. In the classification scheme suggested in this TAG this requirement would apply to any Class 1 SSCs.

Engineering principles: design for reliability	Single failure criterion	EDR.4
During any normally permissible state of plant availability, no single random failure, assumed to occur anywhere within the safety systems provided to secure a safety function, should prevent the performance of that safety function.		

5.6.6 STEP 2 – REFINEMENT

5.6.6.1 The second step of classification incorporates a number of remaining aspects as shown in Figure 4. As with categorisation, this outline classification scheme does not provide detailed guidance and the factors identified below should be seen as triggers for further understanding of the licensee's own arrangements.

5.6.6.2 One factor is (c) the potential for the SSC itself to initiate a fault or exacerbate the consequences of an existing fault. In particular, it is important to ensure that a safety system or safety-related system is not undermined by a lower classification auxiliary service or other support feature. Auxiliary services that support components of a safety or safety-related system should be considered part of that system and should be classified accordingly unless failure does not prejudice successful delivery of its safety function. As such considerations relate to the system design and the mode of failure, this factor is expected to be usually included as part of SSC classification rather than safety function categorisation.

5.6.6.3 A further factor is (d) the time following any initiating fault at which, or the period throughout which, the item will be called upon to operate. These aspects are closely associated with, and may already have been incorporated within, the stable, safe state

considerations of the underlying safety function (see Section 5.5.3). However, they may also depend on the system design (e.g. the ease at which failures could be fixed) and are therefore also included here as part of SSC classification.

5.6.6.4 It may be necessary to improve the reliability of a safety system or safety-related system, or provide further systems (e), in order to achieve an ALARP position with respect to all of the SAPs fault analysis numerical targets [see Ref. 1]. For example, the categorisation/classification process may have identified the need for a Class 2 SSC, but a higher reliability, which could be driven by an increase to Class 1, may be necessary. Conversely, a reduction in class may be justified in some circumstances. This is an important point: the application of any categorisation and classification process does not automatically mean that the safety measures are either suitable or sufficient, nor that the remaining risks have been reduced to ALARP. Ultimately, an effective and correctly implemented process should go a long way to meeting these requirements but it cannot be presumed that this alone is enough.

5.6.6.5 The link between reliability and class of the SSC is presented in Section 5.2.4 of this TAG. Further guidance on the classification of SSC is provided in 5.7 of this TAG.

5.6.6.6 Probabilistic safety analysis (PSA) can be used to inform the design process and help ensure safe operation including supporting the categorisation and classification process particularly for borderline cases and situations in which ALARP considerations are important. This can include an assessment of the reliability of safety measures. Further guidance on PSA is contained in Ref. 11.

5.7 SSC STANDARDS

5.7.1 CROSS-DISCIPLINE ASPECTS

5.7.1.1 SSC classification is undertaken to ensure functional correctness (i.e. the process of ensuring correct requirements capture and design). Classification also helps to ensure that the aspects of the facility design involved in safety or safety-related systems are consistent with the appropriate degree of confidence required against the delivery of the safety functionality. This is achieved by using the SSC class to inform the standards and RGP associated with designing, manufacturing, constructing, installing, commissioning, quality assuring, maintaining, testing and inspecting the item.

5.7.1.2 The approach used should:

- reflect the functional reliability of the SSCs and be suitable for their safety classification;
- ensure the adoption of appropriate national and international nuclear specific codes and standards for Class 1 and Class 2 SSCs. For Class 3 appropriate non-nuclear specific codes and standards may be applied;
- ensure that codes and standards are evaluated to determine if they are suitable and sufficient. Where necessary these standards and codes should be supplemented as necessary to a level commensurate with the importance of the safety function being performed;
- ensure that the amalgamation of different codes and standards for a single aspect of a safety system or safety-related system is either avoided or appropriately justified to demonstrate compatibility;
- ensure, that where there are no appropriate established codes or standards, an approach derived from existing codes or standards for similar equipment in similar applications is used (ECS.4) [Ref. 1]
- ensure, that in the absence of applicable or relevant codes and standards, the results of experience, tests, analysis, or a combination thereof, is used to demonstrate that an item will perform its safety function(s) to a level commensurate with its classification (ECS.5) [Ref. 1].

5.7.1.3 The following sections contain discipline specific guidance on RGP relating to the classification of safety systems. Where appropriate reference to existing standards and codes are included.

5.7.2 ELECTRICAL, CONTROL AND INSTRUMENTATION STANDARDS

5.7.2.1 International Standard 'Nuclear power plants – Instrumentation and control important to safety – Classification of instrumentation and control functions.' BS IEC 61226:2009 [Ref. 5] was a response to the International Atomic Energy Agency (IAEA) requirement to classify nuclear power plants' control and instrumentation (C&I) according to their importance to safety. The standard specifically aims to:

- provide an approach to categorise C&I functions important to safety depending on their contribution to the prevention and mitigation of postulated initiating events, and to develop requirements that are consistent with the importance to safety of each of the categories; and
- assign specification and design requirements to C&I systems and equipment that performs the categorised functions.

5.7.2.2 The methods of categorisation presented in the standard are primarily based on deterministic safety analysis and complemented by probabilistic methods. The standard establishes criteria and methods to categorise C&I functions into three categories (i.e. A, B and C) depending on their importance to safety. The Category of the safety function then determines the technical requirements for the systems intended to deliver the functionality. These categories align with categories A, B and C used in this TAG.

5.7.2.3 BS IEC 61226 [Ref. 5] gives requirements for each safety function category relating to:

- Functions - basic requirements relating to clear, comprehensive and unambiguous functional requirements; use of structured analysis and the graded use of appropriate codes, guides and standards;
- Technical requirements for C&I Systems to ensure that safety functionality is achieved to the specified reliability. These include requirements relating to:
 - Redundancy / diversity / separation and independence;
 - Common cause failures;
 - Power supply requirements;
 - Testing; and
 - Analysis (e.g. DBA, FMEA).
- The operating environment of the equipment delivering the safety function, and
- Quality assurance through the lifecycle.

5.7.2.4 International Standard 'Nuclear power plants – Instrumentation and control important to safety – General requirements for systems' BS IEC 61513: 2013 [Ref. 10] sets out requirements for C&I systems and equipment used to perform safety functions important to safety. The standard is primarily based around the safety lifecycle of the C&I system and covers both architectural and specific system design requirements.

5.7.2.5 The current versions of both BS IEC 61226 [Ref. 5] and BS IEC 61513 [Ref. 10] relate to nuclear power plants. However, it is the intention of the IEC to extend the scope of these standards in the future to cover all nuclear facilities. In the meantime, although not dealing specifically with categorisation or classification, non-nuclear power plants should be assessed using BS IEC 61508:2010 'Functional safety of electrical/electronic /programmable electronic safety-related systems' [Ref. 12]. This standard sets out a generic approach for all safety lifecycle activities for C&I systems used to perform safety functions. Further guidance on ONR's expectation in relation to safety systems is contained in the following Technical Assessment Guidance:

- NS-TAST-GD-003 Safety systems [Ref. 3];
- NS-TAST-GD-046 Computer Based Safety Systems [Ref. 13].

5.7.3 MECHANICAL ENGINEERING STANDARDS

5.7.3.1 Engineered structures, systems and components (SSCs) need to be designed to deliver their required safety functions with adequate reliability, according to the magnitude and frequency of the radiological hazard, and so provide confidence in the robustness of the overall design. The functionality requirements and classification are defined outputs of deterministic and probabilistic safety analysis. The classification of the SSC influences the whole project life cycle, including for example the:

- design approach;
- concept qualification;
- level of auditable design substantiation;
- applied codes and standards;
- material selection;
- procurement phase, detailed design, fabrication, inspections and factory acceptance tests;
- site construction and commissioning phase;
- operational phase in-service EIMT; and
- decommissioning.

5.7.3.2 The diverse range of mechanical engineering SSCs makes it difficult to specify generic codes, standards, and procedures to an assigned nuclear safety classification. In general, there are no UK nuclear specific codes and standards that define the requirements for the categorisation and classification of mechanical engineering aspects. This places the responsibility on the robustness of the assigned quality management arrangements to satisfy the required SSC reliability. The implementation of a robust design process is important as it is the starting point to secure a successful design, which should also be integrated with the safety case production process.

5.7.3.3 The ability to secure the design basis is reliant on the adherence to the established design process. The level of design substantiation and supporting quality arrangements should be commensurate with the assigned classification.

5.7.3.4 An individual SSC is likely to require specific standards and procedures (either industry recognised or specifically generated in-house) and a commensurate quality management plan. If seismic qualification of mechanical plant is needed a seismic classification procedure will need to be developed similar to that applied to civil engineering structures. The classification procedure should include dependencies based on the required performance of the plant during and immediately after the earthquake, including any requirement for operator intervention. If functioning of mechanical plant is dependent on the seismic response of the supporting civil structures (for instance the structures might be required to remain elastic or deformations might be limited to those that the mechanical plant can safely tolerate) then seismic safety functions will need to be generated and categorised by the mechanical engineers to be placed on the civil engineering structures.

5.7.3.5 ONR inspectors are expected to use judgment to determine if the duty holders arrangements are adequate to provide evidence that the level of substantiation for an SSC is commensurate with its classification.

5.7.3.6 Annex 2 of this document sets out mechanical engineering examples of design substantiation considerations and specific standards applicable for nuclear lifts. Further guidance to assist inspectors is set out in ONR Technical Assessment Guides:

- NS-TAST-GD-077 “Procurement of nuclear safety related items or services” [Ref. 14];
- NS-TAST-GD-057 “Design safety assurance” [Ref. 15];
- NS-TAST-GD-079 “Licensee design authority capability” [Ref. 16];
- NS-TAST-GD-049 “Licensee use of contractors and intelligent customer capabilities” [Ref. 17].
- NS-TAST-GD-056 “Nuclear Lifting Operations” [Ref. 18]

5.7.4 STRUCTURAL INTEGRITY STANDARD – NUCLEAR PRESSURE EQUIPMENT DESIGN AND CONSTRUCTION

- 5.7.4.1 Categorisation and classification of SSCs influences the level of assurance provided by the design and manufacturing standards. It is therefore appropriate to consider the impact of the SSC classification and the design and manufacturing standards applied to SSCs to ensure the risk of failure is ALARP.
- 5.7.4.2 Nuclear pressure vessel design and construction (PVDC) codes, such as ASME III [Ref. 19] and RCC-M [Ref. 20] set out a range of requirements for the design and construction of pressure vessels and associated pressure retaining components such as pipework and valves. The requirements are graded according to which of the PVDC code classes are specified for the component. ASME Class 1/M1 components are designed, constructed and inspected to higher standards than ASME Class 2/M2 and likewise to ASME Class 3/M3. The PVDC code class specified for the component also determines the through life inspection regime for the component. Whilst the PVDC codes provide rules for design and construction against these different PVDC code classes, they do not provide the criteria for allocating the PVDC code class that should be specified for a particular component.
- 5.7.4.3 UK experience of categorisation and classification of SSCs includes the categorisation of nuclear pressure equipment (NPE) for pressurised water reactors. Previously NPE has been sub-divided into one of the three nuclear pressure vessel classes in accordance with ANSI N18.2 [Ref. 21]. It is worth noting that these rules mean that NPE in Safety Class 1 are further sub-divided into the three nuclear pressure vessel classes. ANSI N51.1 [Ref. 22] supersedes ANSI N18.2, but this has itself now been withdrawn, but still provides useful guidance. The current approach taken in the US is defined in the Nuclear Regulatory Commission (NRC) Guide 1.26 [Ref. 23] which provides component classification using the function of the component to define the required quality level, which then leads to the nuclear pressure vessel class being set for the component.
- 5.7.4.4 Alternative approaches can be used to determine the PVDC code class. For example, modern design of nuclear power plant has utilised a methodology where the allocation of pressure vessel class is based on the safety class of the component and the radiological barrier role the component performs. It is the ONR’s view that the emphasis is on the licensee to justify any change in safety classification and PVDC code classification from that of previous UK experience to ensure that an appropriate design and manufacturing standard is adopted for the given safety function.
- 5.7.4.5 The SAPs [Ref. 1] recognise that there are situations where it is not possible to show that the consequences of failure are acceptable in the deterministic case. An example would be the reactor pressure vessel in a light water reactor. These are termed the “highest reliability” components. This is an onerous route to constructing an adequate safety case as the likelihood of gross failure of an SSC needs to be shown to be significantly lower than can be shown by compliance with a design code alone. Such components rely on design code compliance as a starting point for the demonstration of integrity, but require additional design and manufacturing quality assurance activities

to provide the required level of confidence in the ability of the component to deliver its safety function through-out its life.

5.7.4.6 Thus the highest reliability components form a distinct and important sub-set of SSCs and SAPs EMC.1 to 3 and paragraphs 286 to 296 [Ref. 1], gives guidance on such situations and the level of demonstration required to make a highest reliability claim.

5.7.5 CIVIL ENGINEERING SYSTEM STANDARDS

5.7.5.1 There are no specific standards within the civil engineering area which discuss categorisation and classification. Inspectors should seek to ensure that licensees have used appropriate processes to determine the categorisation and classification of civil SSCs, as discussed earlier in this guide.

5.7.5.2 For safety related civil engineering standard, it is common to supplement the safety classification with a performance-based classification scheme, especially for seismic hazard withstand, where it is common to have a dual classification for key structures indicating not only their safety classification but also their seismic classification. Seismic classification is typically of three types:

- Seismic class 1 – remains fully functional during and after a design basis event;
- Seismic class 2 – does not collapse during a design basis event and retains limited functionality following an event;
- Seismic class 3 – no specific seismic design.

5.7.5.3 Seismic classification schemes can also include containment functions relating to water tightness and/or air tightness during and following an earthquake. Also seismic safety functions applicable to civil engineering structures may be generated by other disciplines (see Section 5.7.3).

5.7.5.4 It is common to find mixed classifications for structures. For example, the overall enclosure may be class 1, seismic class 1, however sub-structures in the main structure may be classified at lower levels. Careful scrutiny is needed to ensure that the potentially dissimilar behaviour of connected items is catered for in the design and reflected in the safety case claims.

5.7.5.5 The link to design standards from classification requires careful consideration, as specific rules do not exist within design standards. The following provides a brief overview of ONR's SSC classification expectations relating to civil engineering.

- Class 1 – the design will be undertaken using nuclear specific standards, or standards which can be shown to deliver an equivalent reliability. Structures are typically expected to remain elastic under design basis loads. Detailing of the structures should be such that beyond design basis behaviour is ductile and predictable;
- Class 2 – the design will be undertaken using standards which deliver the reliability commensurate with the safety claims made;
- Class 3 – the design will be undertaken using normal industrial standards.

5.7.6 MANAGEMENT SYSTEM AND HUMAN RELIABILITY STANDARDS

5.7.6.1 The classification of SSCs should be considered when determining the supply chain controls that need to be applied when procuring relevant items and services, e.g. specification, supplier capability assessment, inspection and verification, etc. It is not the only consideration however, and care must be taken to avoid over specifying items that may have been assigned a higher classification but are relatively simple, proprietary items, e.g. panel bulbs, cable clips, fuses, structural connections etc.

5.7.6.2 Guidance in the graded application of supply chain controls is in NS-TAST-GD-077 [Ref. 14]. ONR's expectations for proportionate substantiation of operator actions are outlined in NS-TAST-GD-063 Revision 2 – Human Reliability Assessment. [Ref. 8]

6. REFERENCES

1. Safety Assessment Principles for Nuclear Facilities. 2014. Revision 0. November 2014. <http://www.onr.org.uk/saps/index.htm>
2. Licence condition handbook. Office for Nuclear Regulation. <http://www.onr.org.uk/silicon.pdf>
3. NS-TAST-GD-003 Safety systems.
4. NS-TAST-GD-035 Limits and conditions for nuclear safety (operating rules).
5. BS EN IEC 61226: 2010 Nuclear power plants – instrumentation and control important to safety – classification of instrumentation and control functions.
6. Safety Classification of Structures, Systems and Components in Nuclear Power Plants. IAEA Safety Standards Series SSG-30 Subject Classification: 0603-Nuclear power plants.
7. WENRA safety reference levels for existing reactors – September 2014 2014/09/19.
8. NS-TAST-GD-063 Human reliability assessment
9. NS-INSP-GD-022 LC22 Modification and experimentation on existing plant
10. BS EN IEC 61513:2013 Nuclear power plants – instrumentation and control important to safety – general requirements for systems
11. NS-TAST-GD-030 Probabilistic safety analysis
12. BS EN IEC 61508:2010 Functional safety of electrical / electronic / programmable electronic safety-related systems
13. NS-TAST-GD-046 Computer based safety systems
14. NS-TAST-GD-077 Procurement of nuclear safety related items or services
15. NS-TAST-GD-057 Design safety assurance
16. NS-TAST-GD-079 License design authority capability
17. NS-TAST-GD-049 Licensee use of contractors and intelligent customer capability
18. NS-TAST-GD-056 Nuclear Lifting Operations
19. ASME Boiler and Pressure Vessel Code, Section III Rules for Construction of Nuclear Facility Components, American Society of Mechanical Engineers – ASME, New York, 207 Edition
20. RCC-M, design and Construction Rules for Mechanical Components of PWR Nuclear Islands, 2007 Edition. Published by the French Association for design, Construction and In-Service inspection Rules for Nuclear Island Components, AFCEN, Paris
21. Nuclear Safety Criteria for the Design of Stationary pressurised Water Reactor Plants – American Nuclear Society Standards ANSI N18.2 – 1, 1973
22. Nuclear Safety Criteria for the Design of Stationary pressurised Water Reactor Plants – American Nuclear Society Standards ANSI N51.1 – 1, 1983
23. United States Nuclear Regulatory Commission, Regulatory Guide 1.26, Quality Group Classification and Standards for Water-, Steam-, and Radioactive-waste-containing Components of Nuclear Power Plants, March 2007 24.

7. GLOSSARY AND ABBREVIATIONS

ALARP	As low as reasonably practicable
BSL	Basic safety level
BSO	Basic safety objective
C&I	Control and instrumentation
DBA	Design basis analysis
ECS	Engineering safety classification and standards SAPs
EDR	Design for reliability SAPs
EHF	Human factors SAPs
EIMT	Examination, inspections, maintenance and testing
EKP	Engineering key principles SAPs
EMC	Integrity of metal components and structures SAPs
EPE	Chemical (process) engineering SAPs
ERC	Reactor core SAPs
ff	failure frequency
FMEA	Failure modes and effects analysis
FOAK	First of a kind
GDA	Generic design assessment
HAZOP	Hazard and operability study
IAEA	International Atomic Energy Agency
LC	Licence condition
NDT	Non-destructive testing
NPE	Nuclear pressure equipment
NRS	United States Nuclear Regulatory Commission
ONR	Office for Nuclear Regulation
pdf	Probability of failure on demand
PSA	Probabilistic safety analysis
PVDC	Pressure vessel design and construction
PWR	Pressurised water reactor
RGP	Relevant good practice
RPV	Reactor pressure vessel
SAA	Severe accident analysis
SAP	Safety assessment principle(s)
SFR	Safety functional requirement
SMDC	Safety mechanism, devices and circuits
SSC	Structure, system and/or component
TAG	Technical assessment guide(s)
WENRA	Western European Nuclear Regulators' Association

8. ANNEX 1 - EXAMPLES

8.1 BASIS FOR EXAMPLES

- 8.1.1 The following examples seek to present some insights into how safety function categorisation and SSC classification may be reasonably applied. The categorisation and classification processes from Sections 5.5 and 5.6 are used as the basis for the scenarios presented, which attempt to illustrate some of the key concepts, possible approaches and potential pitfalls.
- 8.1.2 The examples do not necessarily reflect the outcome of previous ONR assessments of similar situations nor do they set any precedent in terms of any future scenarios. They present simple, incomplete scenarios to help an ONR inspector understand the issues explored within the TAG.

8.2 RADIOISOTOPE SHIELDING TANK WATER FILTER SYSTEM: SAFETY FUNCTION BREAKDOWN AND LEVEL OF CLASSIFICATION

- 8.2.1 This example explores the breakdown of some preventative safety functions at levels 1 and 2 of the hierarchy of defence in depth and the level at which classification is applied to the safety-related SSCs delivering these functions as part of normal operation.
- 8.2.2 Consider a water-shielded tank storing sealed, non-heat generating radiography sources. Imagine that the tank has a water treatment system that takes off some water, pumps it through a filter and returns it to the tank. This system may have the following two preventative safety functions associated with normal operation:
- sample and maintain the water quality;
 - maintain the watertight integrity of the water treatment system.
- 8.2.3 Let us suppose that, if the first function is not maintained, then some limited source corrosion could occur over a period of time and that a small dose may result if an operator inhaled or ingested some of the contaminated water. On the basis of these consequences, the first safety function could turn out to be Category C. Let us imagine that the second function is Category A, as a loss of the shielding water could quickly lead to a fatal radiation dose to an operator.
- 8.2.4 The identification and categorisation of the two distinct safety functions undertaken by the water treatment system is limited. In this case, to avoid needlessly over-classifying all the components of the water treatment system as Class 1 (as the principal means of delivering an identified Category A function) further breakdown will enable a more sensible classification of the individual SSCs.
- 8.2.5 In this case, only the elements of the system that provides the Category A watertight integrity function (e.g. flanges, pipework, break-in seals for the sensors and the pump body) need be Class 1. Items such as the pump impeller, filter element, measurement sensors and control system may only need to be Class 3 in respect of providing their Category C function.

8.3 ELECTRICALLY-POWERED FURNACE: CLASSIFYING SYSTEMS AND THE TREATMENT OF PROTECTION VERSUS MITIGATION

- 8.3.1 This example explores the approaches and potential pitfalls associated with identifying and classifying protective and mitigative safety systems.
- 8.3.2 Consider an electrically-powered furnace used to heat radioactive material. In the event of an overheating fault, perhaps due to a fault in the control system, a protective

safety function might be “detect an overheating fault and disconnect the power supply”. Imagine that if this function is not delivered, then the furnace could rupture and fatally contaminate the operator. Let us suppose that, given this, the function has been designated as Category A because the overheating furnace could melt the radioactive material and fail, leading to a large airborne release of contamination. The safety system delivering this function would include the temperature sensors, signal processing, trip logic, actuation signal and contactors to disconnect the power supply. This collection of SSCs may then be classified as the Class 1 principal protective safety system providing the Category A function.

- 8.3.3 Let us suppose that an additional, diverse protective safety system exists for the overheating fault. Imagine that this consists of a set of thermal fuses which have been designed to melt should the temperature exceed the trip point of the over-temperature trip safety system described in the previous paragraph. This system is able to safely terminate the fault sequence if the over-temperature protection system fails to respond. As the second protective measure, it might be designated as Class 2 by the classification process.
- 8.3.4 An alternative approach in this case may be to undertake a further breakdown in the original safety function to identify two separate sub-functions met by the two protective systems. In this approach, the Class 1 trip system addresses the first sub-function, but rather than considering the thermal fuse as a second line of delivery of the overarching safety function, it could instead be treated as the principal means of delivering the second sub-function. This is likely to result in the same Class 2 determination because the frequency at which the second sub-function is demanded is reduced by the pfd of the over-temperature trip that is delivering the first function.
- 8.3.5 Now consider that there are additional safety systems that are able to mitigate the radiological consequences. In this example, for instance, they may be a fire detection and alarm system or continuous air monitors that can warn the operator to evacuate. Additionally, the furnace might be located in a filtered containment cell. Such mitigating measures should usually be approached using the categorisation and classification approaches described above for the protective measures. In this example, they may both be Class 3 based on their position in the defence in depth.
- 8.3.6 The potential difficulty that inspectors should look for in this example is where the protective (over-temperature trip and thermal fuses) and mitigative (fire alarm and containment) safety systems are lumped together and considered as a single “overall system” delivering the high level safety function of: prevent an overheating fault from releasing radioactivity. Although this “overall system” should be a Class 1 provision in this example, it has inappropriately combined distinctly different systems and both protective and mitigative elements. The key pit fall occurs if it is argued that the overall Class 1 standard can be built-up from lower standards in each of the different items.
- 8.3.7 This approach should be viewed with caution (see Section 5.6.3 and Ref. 3). It could be avoided by ensuring a sufficiently detailed safety function breakdown and the classification of the clearly distinct safety systems as separate entities rather than as an agglomeration. Classifying combinations of systems should be limited to those situations in which the systems involved have features that might make them susceptible to common-cause failure.

8.4 VERY LOW POWER ASSEMBLY REACTIVITY CONTROL: PREVENTION VERSUS PROTECTION AND APPROPRIATE CLASSIFICATION

- 8.4.1 This example explores a situation in which it is appropriate to place the focus on fault protection rather than prevention due to the practicalities of the engineering design.

- 8.4.2 Consider the on-going control of reactivity in a very low power experimental reactor. Suppose the assembly is water-moderated and is designed to undertake measurements on a variety of neutron flux distributions and to this end it has a number of control rods all under fine computer control. Separate and independent from the normal operation control system is a primary protection system. This has a number of diverse inputs including monitoring for excessive neutron flux. Upon recognising an unsafe condition, the protection system removes the power supplies to electromagnets holding the control rods allowing them to fall into the assembly. In addition, a secondary protection system is provided. Let us suppose that this system receives a diverse flux monitoring signal. If it detects an unsafe condition it opens valves to rapidly drain the moderator and shutdown the reactor. Either of the two protection systems is able to fully shutdown the assembly independently of whether the other acts.
- 8.4.3 In this example, let us suppose that the safety function breakdown has identified a Category A safety function for the control of reactivity under all circumstances on the basis of the risk to an operator. The normal operation control system has been identified as a safety-related system preventing the loss of control. As it is in essentially continuous use the initial classification of the reactivity control system should be a Class 1 with the primary and secondary protection systems as Class 2 and Class 3 respectively.
- 8.4.4 If it can be shown that the use of the computer-controlled normal operation system is unavoidable but that reaching the reliability requirements of a Class 1 system using complex technology is not practicable, then one possible approach may be to reduce the classification of the control system (e.g. to Class 3) and to commensurately increase the classification of the protection systems (e.g. to Class 1 and 2 respectively). This could be justified within the refinement step in the proposed classification scheme.
- 8.4.5 This approach recognises the increased prominence of the protection system in the delivery of the safety function, given the increased expected frequency of the fault condition arising from failure of the normal operation system resulting from the reduction to Class 3. This is consistent with the role of classification in expressing the weight being placed upon the different SSCs.
- 8.4.6 This example has focussed on the need to maintain the control of reactivity through the operation of the normal rod control system. There may of course be other reactivity insertion faults that could occur regardless of the normal control system. The safety function in the event of such faults may independently drive Class 1 and Class 2 requirements for the primary and secondary protection systems.

8.5 POWER REACTOR DECAY HEAT REMOVAL: PRACTICAL CLASSIFICATION OF MULTIPLE LINES OF PROTECTION

- 8.5.1 This example, following-on from the previous scenario, explores some of the acceptable ways in which SSC classification can be adjusted based on the engineering practicalities of fault protection.
- 8.5.2 Consider the removal of decay heat in a pressurised water reactor (PWR) following a fault affecting the normal operation system. As the consequences are likely to be severe and the fault may occur relatively frequently, let us suppose that the safety function of “restore decay heat removal following normal operation system failure” is Category A. Furthermore, let us suppose that the fault analysis (and the comparison against numerical targets and RGP) is such that two independent safety systems are needed in the delivery of this safety function.
- 8.5.3 Imagine that the PWR is under design and that two protective safety systems have been put forward. The first, System X, consists of redundant pump-driven cooling

loops separate to the normal operation system and supported by diesel generators. The second, System Y, is a passive system that, following the opening of some valves, enables heat to be rejected through natural circulation. Either system can remove the maximum decay heat load independently of whether the other system operates.

- 8.5.4 Let us assume that System X has been configured such that it will be called upon before System Y because its use will impose less thermal stress on the facility such that it will have fewer implications for the restoration of normal operation following the fault. System X, however, despite the incorporation of redundancy into its components, is not as reliable as System Y. This passive system has been shown to be highly effective, although its use will subject the plant to a significant transient that may preclude a return to service.
- 8.5.5 Typically, the first protective safety system to act, System X, would be identified as a Class 1 SSC with System Y, as the second line of protection, being identified as Class 2. However, noting the practicalities of the engineering and reliability explained in the previous paragraph, it would be acceptable to reverse this classification. System X could be appropriately claimed as Class 2, despite its use earlier in the fault sequence, whilst System Y is ascribed Class 1.
- 8.5.6 This example is similar, but not identical, to the interchange of class between prevention and protection discussed in Section 5.6.4 and explored in the previous example. It must be undertaken with appropriate justification driven by the engineering practicalities, as it goes against the principle that the focus should be on intervening as early as possible in the development of a fault sequence.

9. ANNEX 2 - FURTHER GUIDANCE ON CLASSIFICATION OF MECHANICAL SYSTEMS

- 9.1 Table below sets out example considerations, by design phase that can affect the delivery of an adequate SSC.

Design Phase	Safety Classification 1&2 SSCs' Design Substantiation Evidence Considerations	Safety Classification 3 SSCs' Design Substantiation Evidence Considerations
Conceptual Design/ Scheme design (SSC Concept design intent demonstration)	<ol style="list-style-type: none"> 1. Design process robustness; guidance set out in ONR Guide TAG Design Safety Assurance NS-TAST-GD-057 [Ref. 15]. 2. Safety analysis; undertake appropriate deterministic and probabilistic safety analysis. 3. Optioneering studies; to reduce risks to ALARP; example of activities include: design reviews, risk assessment and FMEA; HAZOP studies etc. 4. Research and development; undertake appropriate R&D activities to validate / substantiate a first of a kind (FOAK) concept. 5. SSC concept qualification tests. These should confirm an SSC performs its defined safety function(s) for all normal operational, fault and accident conditions identified in the safety case and for the duration of their operational lives. 6. Concept design justification/acceptance report. This should set out the concept design audit trail; claims; arguments and evidence. 	<ol style="list-style-type: none"> 1. Design process robustness; guidance set out in ONR Guide TAG Design Safety Assurance NS-TAST-GD-057 [Ref. 15]. 2. Safety analysis; undertake appropriate deterministic and probabilistic safety analysis. 3. Optioneering studies; to reduce risks SFAIRP; example of activities include: design reviews, risk assessment etc. Providing the design basis is met output broadly establishes the use of industry proprietary SSCs. 4. Codes and standards; absence of appropriate nuclear industry specific codes or standards, broadly establishes the adoption of appropriate industrial codes or standards. 5. Asset management; selection of industry proprietary equipment broadly establishes the supplier's recommended EIMT regime. 6. Procurement arrangements; guidance set out in TAG Supply chain management arrangements for the procurement of nuclear safety related

	<ol style="list-style-type: none"> 7. Codes and standards; adoption of : <ol style="list-style-type: none"> a. specific nuclear codes and standards, (e.g. ASME; NOG etc.) and b. specific in-house guidance and quality management excluded from specific nuclear codes and standards. 8. Asset management; establishment of a commensurate concept asset management regime. This should set out the concept EIMT; surveillance and condition monitoring regime and considers spatial requirements. 9. Procurement arrangements; guidance set out in TAG Supply chain management arrangements for the procurement of nuclear safety related items or services NS-TAST-GD-077 [Ref. 14]. 	<p>items or services NS-TAST-GD-077 [Ref. 14].</p>
<p>Detailed Design/manufacture (SSC product design intent demonstration)</p>	<ol style="list-style-type: none"> 1. Design authority and intelligent customer presence during procurement; guidance set out in TAGs: <ol style="list-style-type: none"> a. NS-TAST-GD-079 Licensee Design Authority Capability [Ref. 16]; and b. NS-TAST-GD-049 Licensee Core and Intelligent Customer Capabilities [Ref. 17]. 2. Detailed design reviews etc. to reduce risks to ALARP. 3. Asset management; establishment of a commensurate detailed design asset management regime. This should set out detailed design EIMT; surveillance and condition monitoring regime and considers detailed design spatial requirements. 4. SSC tests; e.g.: <ol style="list-style-type: none"> a. product factory acceptance tests; and b. demonstration of specific FOAK EIMT aspects <ul style="list-style-type: none"> • These should confirm an SSC ability to deliver its safety function(s) for all normal operational, fault and accident conditions identified in the safety case and for the duration of their operational lives. 5. Detailed design justification/acceptance report should set out the detailed design audit trail. 6. Life time quality records; examples include: <ol style="list-style-type: none"> a. drawings; b. calculations and FMEA; c. material traceability records; d. material certifications including welding consumables; e. welding , NDT procedures and records; 	<ol style="list-style-type: none"> 1. Life time quality records; examples include: <ol style="list-style-type: none"> a. vendor drawings; b. certificate of conformity; c. declaration of incorporation; d. operating and maintenance manual etc.

	<ul style="list-style-type: none"> f. welder qualification records; g. bending procedures; h. heat treatment records; i. certificate of conformity; j. sub orders; k. operating and maintenance manual; l. inspection reports (including 3rd party independent); m. concessions; n. technical file, o. recommended spares lists; p. quality plans etc. 	
<p>Site installation Commissioning</p> <p>(SSCs design intent demonstration)</p>	<ol style="list-style-type: none"> 1. EIMT demonstrations should confirm the design intent and the requirements of LC 21 “Commissioning”: <ul style="list-style-type: none"> a. installation acceptance tests; b. system tests; c. safety tests; and d. active tests and early operations etc. 2. Life time quality records documentation as required by LC 6 “Documents, records, authorities and certificate”. 3. Design justification/acceptance report should set out the commissioning audit trail and to take account of the requirements of : <ul style="list-style-type: none"> a. LC 21 “Commissioning”; and b. LC 20 “Modification to design of plant under construction”. 	<ol style="list-style-type: none"> 1. EIMT demonstrations should confirm the design intent and the requirements of LC 21 “Commissioning”: <ul style="list-style-type: none"> a. installation acceptance tests; b. system tests; c. safety tests; and d. active tests and early operations etc. 2. Life time quality records documentation as required by: <ul style="list-style-type: none"> a. LC 6 “Documents, records, authorities and certificate”; and b. LC 20 “Modification to design of plant under construction”.
<p>Operations (SSC design intent maintained demonstration)</p>	<ol style="list-style-type: none"> 1. Life time quality records documentation as required by LC 25 “Operational records”. 2. Asset management should set out arrangements that includes EIMT arrangements as required by LC 28 “EIMT”, which include a: <ul style="list-style-type: none"> a. plant maintenance schedule; b. commensurate EIMT, surveillance and condition monitoring regime etc. 3. EIMT arrangements should set out the requirements of LC 29 “Duty to carry out tests, inspections and examinations”. 4. Design justification/acceptance report should take account of: <ul style="list-style-type: none"> a. LC 22 “Modification or experiment on existing plant”; and b. LC 15 “Periodic review”. 	<ol style="list-style-type: none"> 1. Life time quality records documentation as required by: <ul style="list-style-type: none"> a. LC 25 “Operational records”; and b. LC22 “Modification or experiment on existing plant”. 2. Asset management should set out arrangements that includes EIMT arrangements as required by LC 28 “EIMT” which include a.: <ul style="list-style-type: none"> a. plant maintenance schedule; b. commensurate EIMT, surveillance and condition monitoring regime etc. 3. EIMT arrangements should set out the requirements of LC 29 “Duty to carry out tests, inspections and examinations”.
<p>Decommissioning</p> <p>(SSCs design intent demonstration)</p>	<p>SSCs’ design intent and substantiation should be reviewed and updated to set out potential changes in the safety case claims. Asset management throughout care and maintenance period should include arrangements similar to those for operational design intent listed above.</p>	<p>SSCs’ design intent and substantiation should be reviewed and updated to set out potential changes in the safety case claims. Asset management throughout care and maintenance period should include arrangements similar to those for operational design intent listed above.</p>