Office for Nuclear Regulation

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 2		
Date Issued:	July 2019	**Review Date:**	July 2024
Approved by:	R. Exley	Professional Lead – Fault Analysis	
Record Reference:	CM9: 2020/262117		
Revision commentary:	Rev 1: Routine fit for purpose update. Additional detail and clarifications added following feedback from licensees and ONR inspectors. No significant changes from revision 0. Rev 2: Updated Review Period		

TABLE OF CONTENTS

Published 07/19

1. INTRODUCTION

1.1 The Office for Nuclear Regulation (ONR) has established Safety Assessment Principles (SAPs) [Ref. 1], which guide ONR's regulatory judgements and actions in the assessment of safety cases for nuclear facilities. The principles presented in the SAPs are supported by a suite of Technical Assessment Guides (TAGs). These further assist ONR assessors 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, the purpose of which should be to prevent faults arising, to provide protection in the event that prevention fails and to provide mitigation should an accident occur, (see SAP EKP.3 at paragraph 5.2.1.2). The identification and categorisation of safety functions and the identification and classification of structures, systems and components (SSCs) are key activities that are required to support reasonable and balanced implementation of defence in depth.

1.3 Safety function categorisation is the process by which safety functions are categorised based on their significance with regard to safety, (see SAP ECS.1 at paragraph 5.2.3.1). A systematic approach to identification of safety functions should be taken. This should take into consideration normal operating, fault and accident conditions, and should be 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 associated safety functions, (see SAP ECS.2). The classification assigned to a SSC indicates the level of confidence required for it to deliver its safety function. It should be used to determine the standards and relevant good practice (RGP) to which SSCs are designed, manufactured, constructed, installed, commissioned, quality assured, maintained, tested and inspected, (see SAP ECS.3).

1.5 It is ONR's expectation that safety function categorisation should be distinct from, and normally be carried out prior to, SSC classification. It is also important to note that although a number of criteria are typically taken into consideration when selecting and designing SSCs, it is also ONR's expectation that the safety function categorisation and SSC classification process is not influenced by preconceived design solutions.

2. PURPOSE AND SCOPE

2.1 This TAG addresses a complex topic and relates to a number of SAPs and licence conditions (LC). It provides advice to ONR assessors in relation to ONR's expectations regarding the licensee's / requesting party's (RP's) arrangements for identifying and categorising safety functions and identifying and classifying SSCs. The TAG also provides guidance that covers the factors and RGP that should be taken into account when categorising safety functions and classifying SSCs.

2.2 ONR assessors should use this TAG to assess the licensee's / RP's safety function categorisation and SSC classification arrangements during generic design assessment (GDA), the permissioning process for new build and plant modification projects.

2.3 This TAG has been organised to provide the key information early, followed by the supporting detail later:

- Sections 5.1 to 5.5 presents the principles of safety function identification and categorisation, and SSC identification and classification;
- Section 5.6 provides an example of a safety function categorisation scheme. Section 5.7 provides an example of a SSC classification scheme. These sections provides ONR assessors with a starting point from which to judge the adequacy of the licensee's / RP's arrangements;
- Section 5.8 provides discipline specific SSC classification guidance;
- Annex 1 contains examples to illustrate the categorisation and classification process;
- Annex 2 provides further guidance in relation to the classification of mechanical systems.

2.4 This guide is restricted to nuclear safety function categorisation and SSC classification. It does not address the categorisation of documents, maintenance, human actions, engineering changes / plant modification proposals. However, it should be noted that such categorisation should be informed by the safety functions and SSCs to which they relate.

3. RELATIONSHIP TO LICENCE CONDITIONS AND LEGISLATION

3.1 RELEVANT LICENCE CONDITIONS

3.1.1 The following LCs [Ref. 2] are considered relevant to this TAG:

- LC 14 (safety documentation) requires the licensee to develop 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, therefore, set-out the methodology for the identification and categorisation of safety functions, the identification and classification of SSCs, and how this information will be generated, underpinned and used in the production and assessment of the safety case;
- LC 17 (management systems) requires the licensee to establish and implement systems that give due priority to safety and 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;
- LC 23 (operating rules) 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 LC 14. 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;
- LC 27 (safety mechanisms, devices and circuits (SMDCs)) requires the licensee not to operate, inspect, maintain or test its facility unless suitable and sufficient 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 Safety Systems TAG (NS-TAST-GD-003) [Ref. 3]). In line with this TAG, safety functions should be identified and categorised, and SSCs should be identified and classified;

- LC 28 (examination, inspection, maintenance and testing (EIMT)) requires that the licensee makes and implements adequate arrangements for the regular and systematic 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 level of confidence commensurate with the SSC classifications justified within the safety case.

3.2 OVERARCHING UK LEGISLATION

3.2.1 The Health and Safety at Work Act 1974 (HSWA) [Ref. 4] requires employers to ensure the health and safety of their employees and members of the public who may be affected by their undertakings. In relation to this employers are required to demonstrate that all reasonably foreseeable risks associated with their undertakings have been reduced to a level that is as low as reasonably practicable (ALARP). The identification and categorisation of safety functions and the identification and classification of SSCs play a significant role in achieving this.

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

4.1 SAPs

4.1.1 SAP ECS.1 and SAP ECS.2 refer directly to safety function categorisation and SSC classification respectively, (see paragraphs 5.2.3.1 and 5.3.3.1). SAP ECS.3 covers the relationship between SSC classification and codes and standards, (see paragraph 5.3.5.1). This TAG focuses on these principles, although a number of other SAPs, such as key principal SAPs EKP.3-5, are also relevant, (see paragraphs 5.2.1.2, 5.2.2.5 and 5.3.2.2).

4.2 TAGs

4.2.1 This TAG is closely related to the Safety Systems TAG (NS-TAST-GD-003) [Ref. 3], which outlines the key difference between safety-related systems and safety systems, and their design expectations. The Safety Related Systems & Instrumentation TAG (NS-TAST-GD-031) [Ref. 5] also provides additional guidance regarding the relationship between safety-related systems and safety systems.

4.2.2 It should be noted that this TAG adopts a similar approach to that outlined in the Limits and Conditions for Nuclear Safety (Operating Rules) TAG (NS-TAST-GD-035) [Ref. 6], which provides guidance in relation to the identification and implementation of conditions and limits.

4.3 IAEA SAFETY STANDARDS

4.3.1 Several International Atomic Energy Agency (IAEA) documents state that items important to safety should to be identified and classified on the basis of their function and their safety significance, e.g.:

- Safety of Nuclear Power Plants (NNPs): Design (SSR-2/1) [Ref. 7];
- Safety Assessment for Facilities and Activities (GSR Part 4) [Ref. 8];
- Safety of Nuclear Fuel Cycle Facilities (SSR-4) [Ref. 9].

4.3.2 Further relevant guidance is provided within:

- Safety Classification of SSC in NNPs (SSG-30) [Ref. 10];
- Application of the Safety Classification of SSCs in Nuclear Power Plants (NNP) (IAEA-TECDOC-1787) [Ref. 11].

4.3.3 This TAG has taken into consideration, and broadly aligns with, the aforementioned IAEA guidance.

4.4 WENRA REFERENCE LEVELS

4.4.1 Western European Nuclear Regulators Association (WENRA) safety reference levels for existing reactors [Ref. 12] have been considered during the development of this TAG. This states that all SSCs important to safety shall be identified and classified on the basis of their importance for safety. In addition, the WENRA report on the safety of new NPP designs [Ref. 13] sets expectations that safety features specifically designed for fulfilling safety functions required in postulated core melt accidents shall be safety classified.

4.5 INTERNATIONAL SAFETY STANDARDS

4.5.1 The guidance contained in this TAG is consistent with BS IEC 61226 (NPPs – Instrumentation and Control (I&C) Important to Safety – Classification of I&C Functions) [Ref. 14]. BS IEC 61226 deals specifically with the categorisation of safety functions associated with control and instrumentation (C&I) systems and equipment. The principles detailed in BS IEC 61226 are considered relevant to all nuclear facilities (i.e. not just NNPs) and are considered to be applicable to other technical disciplines.

5. ADVICE TO ONR ASSESSORS

5.1 GENERAL

5.1.1 Identification and categorisation of safety functions and the identification and classification of SSCs plays an important role in assuring that appropriate and adequate levels of defence in depth are provided to ensure the safety of the facility. It is important to note that safety function categorisation and SSC classification is often a multi-disciplinary exercise and requires discussion and interaction between various engineering disciplines and fault analysis.

5.1.2 There are five high level objectives that a safety function categorisation and SSC classification process should ensure:

- The systematic identification and categorisation of safety functions;
- The systematic identification and classification of SSCs delivering those safety functions;
- That the principle of defence-in-depth is applied, (with suitable and sufficient prevention, protection and mitigation, in that order);
- That ALARP and RGP continue to always apply;
- That classification informs the entire lifecycle of activities associated with SSCs.

5.1.3 The following sections address the above aspects and provide associated guidance to ONR assessors when assessing licensee's / RP's categorisation and classification arrangements:

- Section 5.2.1 – Definition and purpose of safety functions;
- Section 5.2.2 – Identification of safety functions;
- Section 5.2.3 – Safety function categorisation;
- Section 5.3.1 – Safety systems and safety-related systems;
- Section 5.3.2 – Safety measures and human based safety claims;
- Section 5.3.3 – SSC classification;
- Section 5.3.4 – SSC reliability;
- Section 5.3.5 – Design and lifecycle implications of SSC classification;
- Section 5.4 – The level to apply categorisation and classification;
- Section 5.5 – Facility lifecycle;
- Section 5.6 – Example safety function categorisation scheme;
- Section 5.7 – Example SSC classification scheme;
- Section 5.7.4 – Prevention versus protection;
- Section 5.8 – SSC standards for various engineering disciplines.

5.2 SAFETY FUNCTIONS AND CATEGORISATION

5.2.1 DEFINITION AND PURPOSE OF SAFETY FUNCTIONS

5.2.1.1 A safety function is a specific purpose or objective that must be accomplished in the interests of safety, (see reference 14). It should usually be specified or described with minimal 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 approach should be taken during the design of new plant and when existing plant is modified.

5.2.1.2 Safety functions are used to define the safety purposes and objectives of a nuclear facility during normal operations and during fault or accident conditions. Safety functions should be considered, as appropriate, across all levels of the hierarchy of defence in depth detailed, (see SAP EKP.3 and paragraph 5.2.1.3).

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.		

5.2.1.3 Table 1 below is taken from the SAPs [Ref. 1] and identifies the objective of each of the five levels of defence in depth and means of achieving them. It should be noted that the means of achieving each objective are indicative of the measures that should be taken, and should not be taken as absolute rules.

Level	Objective	Defence / Barrier
Level 1	Prevention of abnormal operation and failure by design.	Conservative design, construction, maintenance and operation in accordance with appropriate safety margins, engineering practices and quality levels.
Level 2	Prevention and control of abnormal operation and detection of failures.	Control, indication, alarm systems or other systems and operating procedures to prevent or minimise damage from failures.
Level 3	Control of faults within the design basis to protect against escalation to an accident.	Engineered safety features, multiple barriers and accident or fault control procedures.
Level 4	Control of severe plant conditions in which the design basis may be exceeded, including protecting against further fault escalation and mitigation of the consequences of severe accidents.	Additional measures and procedures to protect against or mitigate fault progression and for accident management.
Level 5	Mitigation of radiological consequences of significant release of radioactive material.	Emergency control and on and off site emergency response.

Table 1 – Objective of each level of protection and means of achieving them

5.2.1.4 The safety functions that are needed during the normal operation of a facility usually relate to levels 1 and 2 of the hierarchy. They describe the safety functions that are delivered by 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, (see Safety Systems TAG (NS-TAST-GD-003) [Ref. 3]).

5.2.1.5 Those safety functions that are needed in response to a fault or accident condition usually relate to levels 3 to 5 of the hierarchy. They describe the safety functions that are delivered by the safety systems that have been put in place to control faults and to prevent them from escalating beyond the design basis (i.e. level 3) and to mitigate against further escalation and radioactive release should an accident situation arise (i.e. levels 4 and 5).

5.2.1.6 Note that as level 5 measures typically represent emergency responses, they are dominated by non-engineered measures (such as fire services, evacuation, sheltering and iodine prophylaxis) and are often not fully under the control of licensee. As a result, there is reduced value in detailed safety function analysis or SSC classification. Level 5 measures do need to be identified, appropriately sized, maintained, controlled and available for deployment of demand; however, the ONR assessor may consider that the rigorous application of categorisation and classification scheme not to be the best or only way to ensure this.

5.2.1.7 ONR assessors should be aware that safety functions are referred to by some licensees / RPs 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. 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.

5.2.1.8 Safety functions are also sometimes described based on their position with the hierarchy of defence in depth, (e.g. 'duty' or 'preventative' functions / 'fault' or 'protective' functions / 'accident' or 'mitigation' functions).

5.2.2 IDENTIFICATION OF SAFETY FUNCTIONS

5.2.2.1 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.

5.2.2.2 The fundamental safety functions for a nuclear reactor (see paragraph 540 of the SAPs [Ref. 1] and SAP ERC.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.		

5.2.2.3 For non-reactor facilities (see paragraph 159 of the SAPs and SAP EPE.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.		

5.2.2.4 The fundamental safety functions can be broken-down 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. This may identify 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. This 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. This may identify the need to avoid the formation of an explosive atmosphere to prevent a detonation challenging the integrity of a containment building.

5.2.2.5 The above top-down safety function breakdown is a way of achieving the structured identification of safety functions in line with SAP EKP.4. However, there are other ways in which the licensee / RP 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.		

5.2.2.6 It should be noted that the safety function breakdown process should take into consideration normal operations throughout the lifecycle of the facility and fault or accident conditions. The WENRA Reference Levels [Ref. 12] 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.

5.2.2.7 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 5.4 and explored in the examples in Annex 1.

5.2.3 SAFETY FUNCTION CATEGORISATION

5.2.3.1 SAP ECS.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.		

5.2.3.2 It is an expectation of the SAPs that the licensee's / RP's safety function categorisation scheme should be linked explicitly with the design basis analysis (DBA), (see paragraph 160 of the SAPs [Ref. 1]). However, it is also an expectation of the SAPs that probabilistic safety analysis (PSA) and severe accident analysis (SAA) should also be undertaken to ensure that the all relevant failure conditions and all levels of defence in depth are taken into consideration.

Fault analysis: severe accident analysis	Relationship to DSA and PSA	FA.25
The severe accident analysis should be performed in a manner complementary to the DBA and PSA, so that each type of analysis informs the others in a mutually consistent manner within the facility's safety case.		

5.2.3.3 The licensee's / RP's safety function 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 PSA);
- Employ an appropriate number of safety function categories (three categories are recommended by IAEA guidance (see reference 10));
- 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.

5.2.3.4 In line with paragraph 161 of the SAPs, 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;
- The extent to which the safety function is required, either directly or indirectly, to prevent, protect against or mitigate the consequences of initiating faults.

5.2.3.5 As noted in section 5.2.1, the safety functions should be described separately to the engineering means by which they will be delivered. Therefore, safety function categorisation should not usually take into account 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.

5.2.3.6 An example categorisation scheme is given in section 5.6.

5.3 STRUCTURES, SYSTEMS AND COMPONENTS AND THEIR CLASSIFICATION

5.3.1 SAFETY SYSTEMS AND SAFETY-RELATED SYSTEMS

5.3.1.1 The SAPs [Ref. 1] describe an SSC as an item important to safety that provides a safety function. There are two distinct groups:

- 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.

5.3.1.2 Nuclear facilities use a variety of systems concerned with safety. Safety systems are provided to detect potentially dangerous plant failures or conditions and to implement appropriate safety actions, i.e. they are systems that respond to a fault to prevent or mitigate a radiological consequence, and incorporate protection systems, safety actuation systems and the essential services that provide support. These systems generally contribute to levels 3 to 5 of a defence in depth concept.

5.3.1.3 Besides the safety systems identified above there are other systems, known as safety-related systems that perform an operational function but which also provide a claimed safety benefit.

5.3.1.4 Examples of safety-related SSCs include:

- Reactor control rod system;
- Reactor pressure vessel (RPV);
- Condensate polishing systems;
- Reprocessed radioactive material holding vessel.

5.3.1.5 Examples of safety SSCs include:

- Main guard lines;
- Diverse shut down systems;
- Emergency cooling systems;
- Sump level detectors,
- Flammable gas detectors.

5.3.1.6 Both safety systems and safety-related systems should be classified according to the significance of their contribution to the safety functions that they support.

5.3.1.7 For further information on safety systems and safety related systems and the related concepts of protected plant and unprotected plant, see the Safety Systems TAG (NS-TAST-GD-003) [Ref. 3] and the Safety Related Systems and Instrumentation TAG (NS-TAST-GD-031) [Ref. 5].

5.3.2 SAFETY MEASURES AND HUMAN BASED SAFETY CLAIMS

5.3.2.1 SAP ECS.2 (see paragraph 5.3.3.1) focuses on the application of classification to SSCs. However, paragraph 164 of the SAPs [Ref. 1] 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, which states that a systematic approach to the identification of human actions that can impact safety should be taken for both normal operations as well as during fault or accident conditions. SAP EHF.4 states that any administrative controls needed in support of such actions should also be identified, (see the Human Reliability Analysis TAG (NS-TAST-GD-063) [Ref. 15] and Procedure Design and Administrative Controls TAG (NS-TAST-GD-060) for further guidance).

Engineering principles: human factors	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 factors	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.		

5.3.2.2 The term safety measure encompasses both the human actions and SSCs needed in the delivery of safety functions. A safety measure is defined [Ref.1] 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 states that safety measures should be identified against the delivery of the safety functions at all levels of the defence in depth.

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

5.3.2.3 Although this TAG focuses on the classification of SSCs, it is expected that the licensees / RPs 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 / RP may implement a combined approach that classifies complete safety measures.

5.3.3 SSC CLASSIFICATION

5.3.3.1 SAP ECS.2 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.		

5.3.3.2 The licensee's / RP's SSC 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 are recommended by IAEA guidance, (see reference 10));
- 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.

5.3.3.3 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[1] 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;
- 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.

5.3.3.4 Once an SSC has been classified, it is normally assumed that all sub-components of the SSC will 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 into account redundancy, diversity or independence within the overall system design. Section 5.4 and examples in Annex 1 provide further guidance.

5.3.3.5 The detailed approach to SSC classification may depend on the specialist discipline area. For example, the classification process for C&I systems in NPPs is carried out according to BS IEC 61226 [Ref. 14]. Discipline-specific guidance is provided in section 5.8.

[1] The frequency of demand on the safety function is already considered as part of the safety function category so the "probability" here is simply the portion of this experienced by the particular SSC being classified. In Section 5.7.1 we offer a simple approach in which an SSC is judged to either be principal, significant or other in its prominence.

5.3.4 SSC RELIABILITY

5.3.4.1 The class of an SSC is fundamentally linked with its reliability, (this is discussed further in the Safety Systems TAG (NS-TAST-GD-003) [Ref. 3]). Using the three-class scheme recommended by the SAPs [Ref. 1] (expanded on later in this TAG), Table 2 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. Where SSC reliability differs to the expected range, this should prompt further consideration and the difference should be justified. Techniques such as PSA may be of use to identify these cases and support the justification.

SSC Class	Failure frequency per 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 2 – Relationship between SSC class and the failure frequency and probability of failure on demand, (see reference 3)

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

5.3.5 DESIGN AND LIFECYCLE IMPLICATIONS OF SSC CLASSIFICATION

5.3.5.1 The intent of SAP ECS.3 is that the range of lifecycle activities associated with an SSC are controlled by codes and standards appropriate to its classification.

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.		

5.3.5.2 It should be noted that as SSC classification is directly linked to reliability, (see section 5.3.4). It is also 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. 16]).

5.4 THE LEVEL TO APPLY CATEGORISATION AND CLASSIFICATION

5.4.1 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. The SSCs that make up the plant systems can also be broken-down into an increasingly more detailed array of sub-systems and components and 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.

5.4.2 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.

5.4.3 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 then be carried out at the level of detail at which the safety functions have been categorised.

5.4.4 When classifying a group of SSCs as a single item, the group should generally extend to the combination of equipment needed to deliver a particular safety function in a particular way. 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.

5.4.5 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 generally not be included and classified alongside protective safety systems (level 3) as part of an overall ‘system’ which is classified as a single item.

5.4.6 The above guidance intends 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.

5.4.7 Some examples illustrating the typical approach to safety function breakdown and classification and the assignment and classification of SSCs are provided in Annex 1.

5.5 FACILITY LIFECYCLE

5.5.1 The provision of properly defined safety functions and SSCs are fundamental for the development of robust safety cases and well-engineered safety 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 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.

5.5.2 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. 17]):

- ***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 5.2);
- ***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 5.3);
- ***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 5.3 and 5.8);
- ***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 5.2);
- ***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.

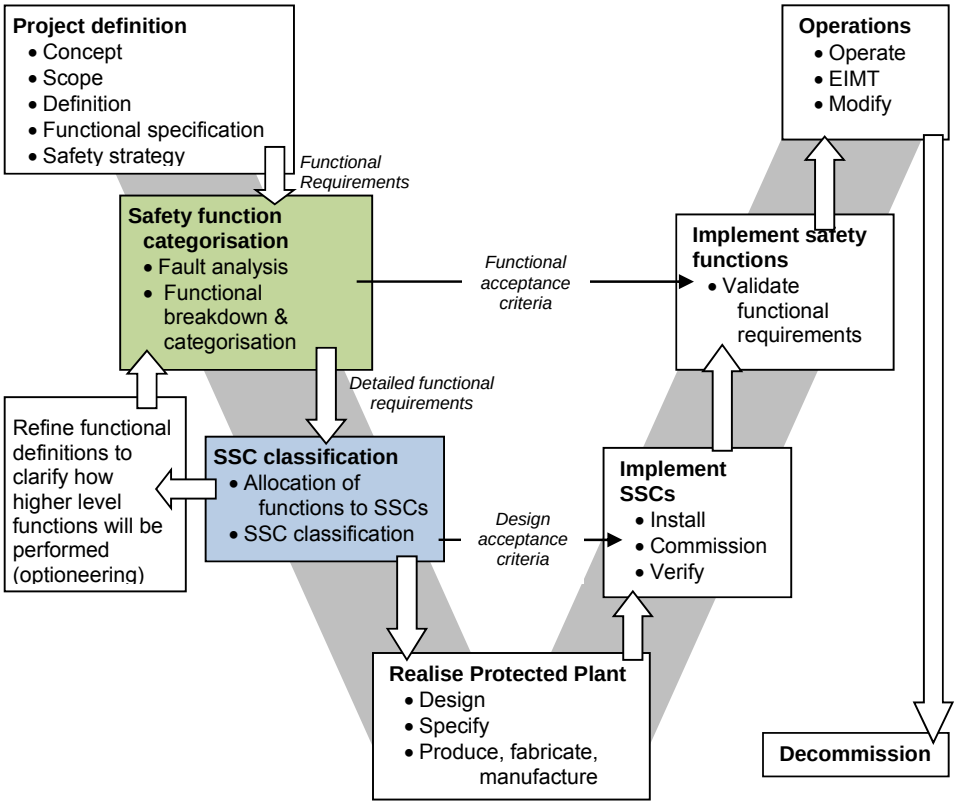

Figure 1 – Role of safety function categorisation (green box) and SSC classification (blue box) within the lifecycle model ('V-diagram')

5.6 EXAMPLE SAFETY FUNCTION CATEGORISATION SCHEME

5.6.1 APPROACH

5.6.1.1 Section 5.2.3 explains the overarching expectations of a safety function categorisation scheme. The licensee / RP 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).

5.6.1.2 This section **outlines** a process that would meet the expectations of SAP ECS.1, (see paragraph 5.2.3.1 and section 5.2). ONR assessors should view it as a **starting point** to inform their assessment of the suitability and sufficiency of the core of the licensee's / RP's arrangements. **It is not a prescribed method and other approaches can be used**.

5.6.1.3 The suggested scheme makes use of the three categories recommended in the SAPs at 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.

5.6.1.4 Figure 2 shows a diagram that draws and expands upon the categorisation factors listed under SAP 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.

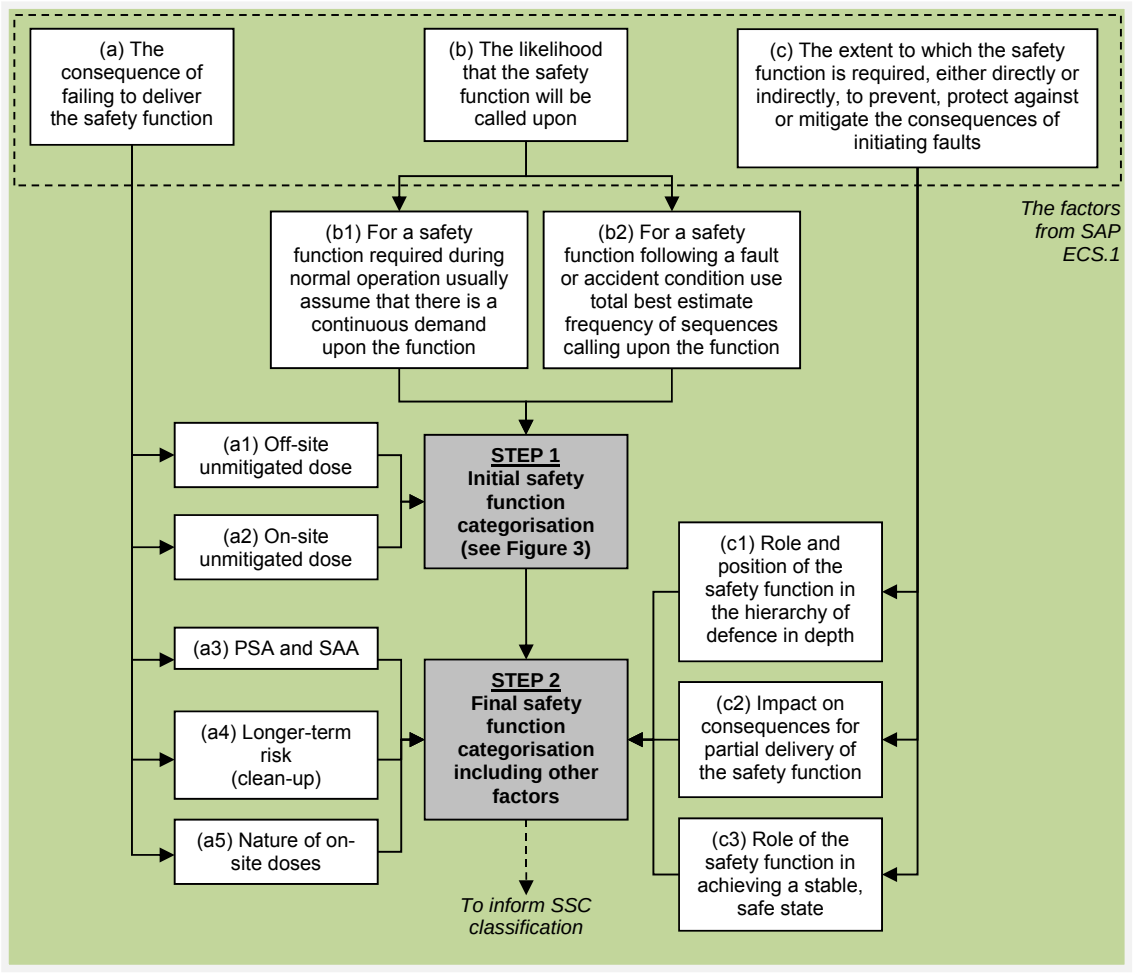

Figure 2 – Safety function categorisation scheme

5.6.2 STEP 1 – INITIAL CATEGORISATION

5.6.2.1 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 are:

(a) The consequences should the safety function not be performed;

(b) The likelihood with which a demand is placed upon the safety function.

5.6.2.2 The consequence (a) of failing to deliver the safety function is interpreted as 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 and this could be re-used appropriately here. 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.

5.6.2.3 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).

5.6.2.4 Figure 3 shows the regions of frequency and consequence, 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.

5.6.2.5 For reference, the basic safety objective (BSO) and the basic safety level (BSL) from SAP Target 4 are included. The regions in figures 3a and 3b are set out as a guide. The regions were arrived at following extensive discussion within and outside ONR for the first revision of this TAG and reflect an average of many licensees / RPs own regions.

5.6.2.6 Should the licensee / RP 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 / RP's arrangements. Two considerations for the ONR assessor should be whether, in general, the approach is delivering design provisions that are consistent with RGP and the needs of the safety case, and in any specific application, that the final SSC provision is consistent with reducing risks to ALARP, (i.e. that it would be grossly disproportionate to do more).

5.6.3 STEP 2 – REFINEMENT

5.6.3.1 The second step involves more qualitative factors. Detailed guidance is not provided here; instead, the factors identified are triggers for further understanding of the licensee's / RP's own arrangements. This is in the context of the nature of the facility in question and the specific safety function being categorised.

5.6.3.2 The qualitative factors suggested include the consideration of (a3) PSA and SAA 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.

5.6.3.3 Consideration could also be made of the nature of on-site doses (a5) including factors such as whether the on-site unmitigated doses affect a large or small number of people, whether these recipients are classified radiation workers, non-nuclear personnel or site visitors and the speed at which the consequences are realised. These aspects may result in a change in the initial safety function categorisation.

5.6.3.4 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 5.7.4.

5.6.3.5 Another factor is (c2) the potential reduction or exacerbation in consequences should there only be partial delivery of the safety function.

5.6.3.6 The last factor (c3) relates to the significance of the safety function in achieving a stable, safe state. This is defined by the SAPs [Ref. 1] 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. Note that this factor is consistent with the approach taken by some licensees and RPs who choose to distinguish between the safety functions placing the plant in a controlled state and the functions required for the longer-term establishment of a shutdown state (from the controlled state), with the latter being designated a lower categorisation. 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.

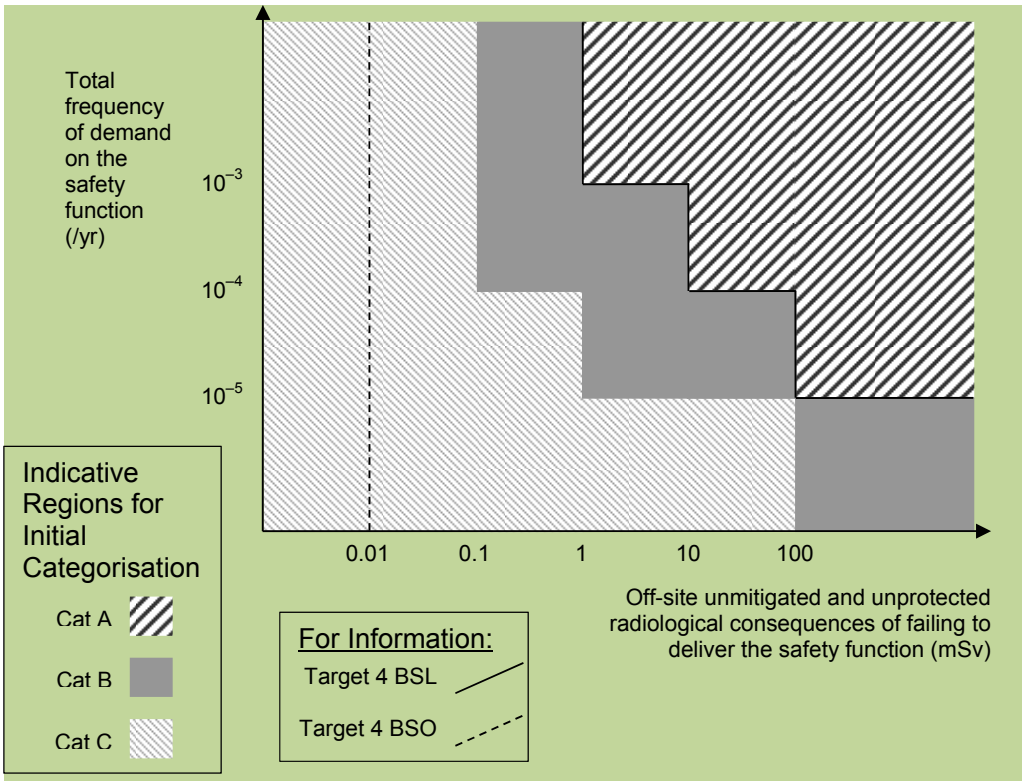

Figure 3a – Off-site frequency / consequence regions for initial safety function categorisation (see section 5.6.2)

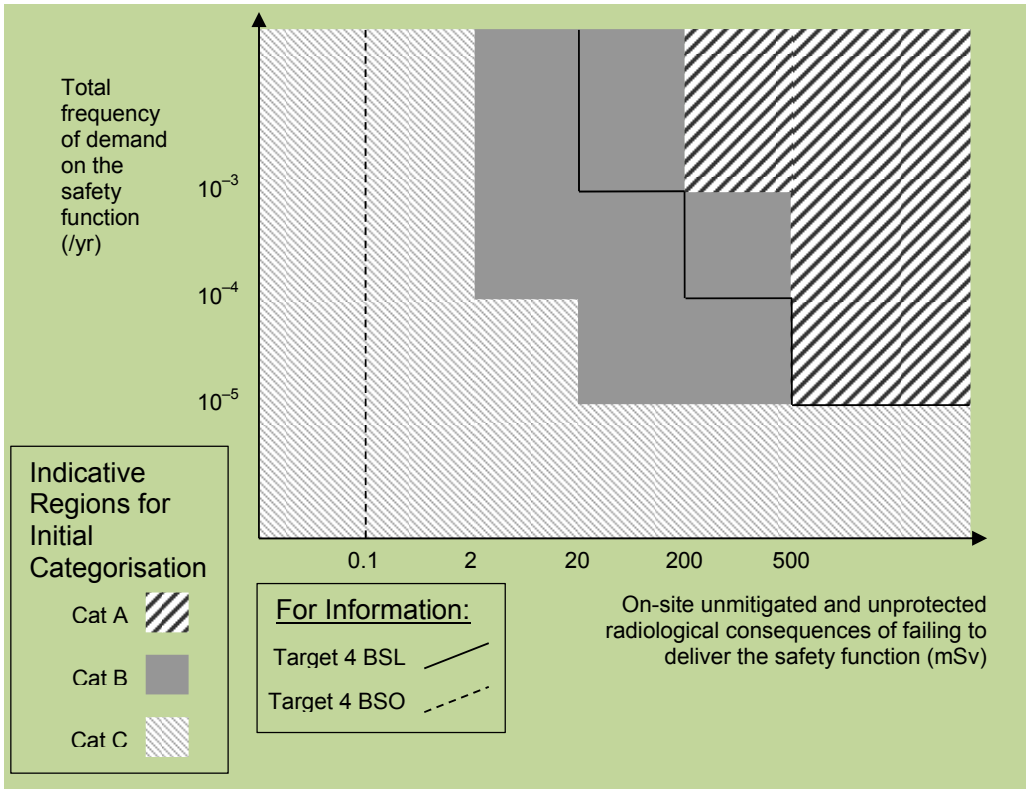

Figure 3b – On-site frequency / consequence regions for initial safety function categorisation (see section 5.6.2)

5.7 EXAMPLE SSC CLASSIFICATION SCHEME

5.7.1 APPROACH

5.7.1.1 This section outlines an SSC classification scheme satisfying the expectations of SAP ECS.2, (see paragraph 5.3.3.1 and section 5.3). It makes use of the three-class scheme recommended in the SAPs at 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.

5.7.1.2 As with the example categorisation process this guidance should be used by ONR assessors as a starting point when assessing the licensee's / RP's arrangements.

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

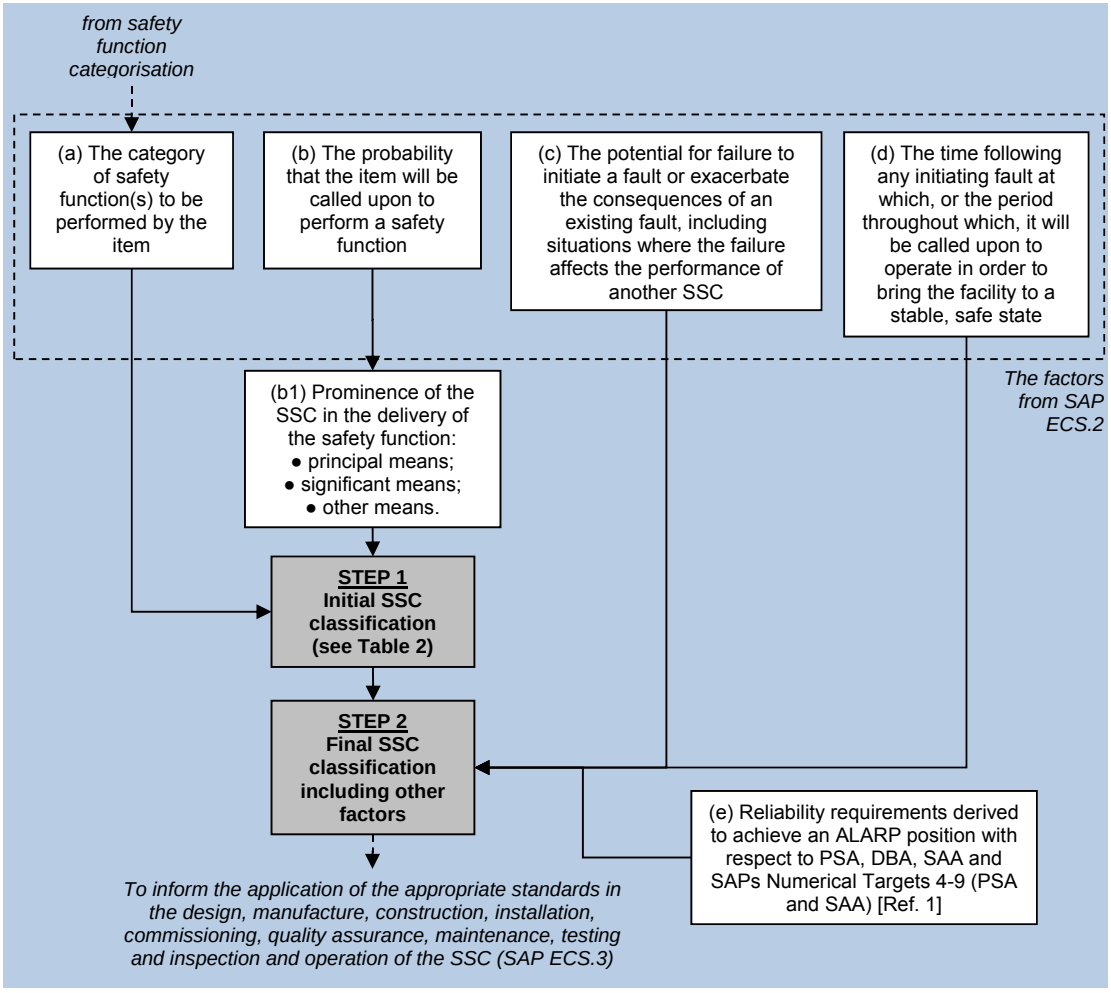

Figure 4 – SSC classification scheme

5.7.2 STEP 1 – INITIAL CLASSIFICATION

5.7.2.1 The first step assigns an initial expectation of the SSC classification using Table 3 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, (see section 5.7.4 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 usually relates to their position in the hierarchy of defence in depth and, often, but by no means always, to the order in which the SSCs respond to the progression of a fault, i.e. first / second / third.

5.7.2.2 The main expectation is that the principal 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 (see reference 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		
		Principal means	Significant means	Other means
	Category A	Class 1	Class 2	Class 3
	Category B	Class 2	Class 3	
	Category C	Class 3		

Table 3 – Initial SSC classification

5.7.2.3 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.

5.7.2.4 It is ONR's expectation that the combinations of categorisation and classification, presented in Table 3 above, should be achieved for new plant. This would represent the modern standard for the assessment of existing plant in any periodic review of safety or for modifications. A robust justification would require demonstration otherwise. Given a strong Class 1 principal means, it may be acceptable in some circumstances to accompany it with a Class 3 significant means to deliver a Category A function. However, this would require an adequate ALARP justification to be made.

5.7.2.5 Typically, it is ONR's expectation that Class 1 and Class 2 SSCs will feature within the safety measures identified for design basis faults. This is because DBA should be applied to faults with unmitigated consequences exceeding the Target 4 BSL [Ref. 1] 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 3). However, ONR expects that (particularly for a modern design) defence in depth is also demonstrated in addition to the safety measures claimed in the DBA. Therefore, additional Class 3 SSCs could be identified as other means to support these functions.

5.7.3 COMBINING SYSTEMS AND SAFETY CLASSES

5.7.3.1 Section 5.4 states 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 break-down the safety functions further and assign different classes to individual SSCs depending on their role in the delivering these more specific functions.

5.7.3.2 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). However, where unavoidable (e.g. where alternative reasonably practicable means of achieving the required functionality or safety performance are not readily available) it may be acceptable to use multiple lower class systems provided that it can be justified that the combination of these systems can achieve the integrity of the original higher class system that was being replaced.

5.7.3.3 Considering separate systems as a single classified combination may be preferable if they are vulnerable to common cause failures, i.e. when there are similarities in location or function. However, section 5.4 states that 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.

5.7.3.4 For the issues discussed above, the use of probabilistic tools and techniques may provide further insight into the risk impacts of different SSC classification combinations. However, it is important to note that an overall level of risk must be demonstrated to be ALARP.

5.7.4 PREVENTION VERSUS PROTECTION

5.7.4.1 The most effective way to maintain safety is to prevent abnormal events and incidents occurring. IAEA SSR2/1 [Ref. 7] states that a design should *"ensure, as far as is practicable, that the first, or at most the second, level of defence is capable of preventing an escalation*". In other words, prevention should be a priority in the application of defence in depth. However, while it may be desirable (and in some cases achievable) to have high class (and, therefore, high integrity) SSCs delivering preventative safety functions, it is not always reasonably practicable to do so.

5.7.4.2 Safety-related normal operation systems can be crucial in preventing an abnormal event escalating. However, they are often too complex (in the case of C&I systems) or too extensive (in the case of pipework or vessels) to make a high safety classification practicable. Instead, it will be protective systems (defence in depth level 3), and very occasionally engineered mitigation systems (defence in depth level 4), which will end up with the highest safety classification. This is acceptable; however, ONR assessors should consider whether the final distribution of safety classifications across all levels of defence in depth is reasonable and balanced (consistent with the focus on prevention over protection / mitigation). It may, therefore, be necessary to seek further evidence from the licensee / RP if this is not adequately justified.

5.7.4.3 There are a number of ways in which the licensee's / RP's arrangements may practically deal with this topic. Whilst ONR does not prescribe an approach, one solution could be to distinguish between preventative and protective functions and amend their categorisation, (see section 5.4). An alternative solution may be to provide further guidance on how principal, significant and other can be interpreted when classifying an SSC.

5.7.5 NUMBER AND QUALITY OF SAFETY SYSTEMS

5.7.5.1 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. Equally, a Class 1 safety system backed-up by a Class 2 safety system may be required, particularly for frequent faults.

5.7.5.2 The assessment of whether the number and quality of safety systems is appropriate and adequate goes beyond the application of categorisation and classification. For example other SAPs [Ref. 1] such as SAP ERC.2 and SAP EDR.4 may be relevant.

5.7.5.3 SAP ERC.2 states 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 to 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.		

5.7.5.4 It is a specific ONR expectation that the single failure criterion, covered by SAP EDR.4, will apply, in all but exceptional circumstances, 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.		

5.7.6 STEP 2 – REFINEMENT

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

5.7.6.2 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.

5.7.6.3 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 5.6.3.4). 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.

5.7.6.4 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 reference 1).
For example, the initial classification step may indicate a Class 2 SSC; however, the need for a higher reliability may necessitate that this is increased to a Class 1 SSC. Conversely, a reduction in class may be justified in some circumstances. This is an important point, as 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 help satisfy these requirements. However, it cannot be presumed that this alone is enough.

5.7.6.5 The link between reliability and class of the SSC is discussed in section 5.3.4. Further guidance on the classification of SSCs is provided in section 5.8.

5.7.6.6 PSA is expected to be used to inform the design process and help ensure safe operation including supporting the categorisation and classification process.

Fault analysis: PSA	Use of PSA	FA.14
PSA should be used to inform the design process and help ensure the safe operation of the site and its facilities.		

5.7.6.7 PSA can provide insight particularly for borderline cases and situations in which ALARP considerations are important. This can include an assessment of the reliability of safety measures and confirmation that the SSC classification results in risks being reduced to ALARP. Further guidance on PSA is contained in the PSA TAG (NS-TAST-GD-030) [Ref. 18].

5.8 SSC STANDARDS FOR VARIOUS ENGINEERING DISCIPLINES

5.8.1 CROSS-DISCIPLINE ASPECTS

5.8.1.1 SSC classification is the process by which SSCs are classified on the basis of their significance in delivering associated safety functions. The classification assigned to a SSC indicates the level of confidence required for it to deliver its safety function. It should be used to determine the standards and RGP to which SSCs are designed, manufactured, constructed, installed, commissioned, quality assured, maintained, tested and inspected.

5.8.1.2 This process 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, (see SAP ECS.4);

Engineering principles: safety classification and standards	Absence of established codes and standards	ECS.4
Where there are no appropriate established codes or standards, an approach derived from existing codes or standards for similar equipment, in applications with similar safety significance, should be adopted.		

- 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, (see SAP ECS.5).

Engineering principles: safety classification and standards	Use of experienced, tests or analysis	ECS.5
In the absence of applicable or relevant codes and standards, the results of experience, tests, analysis, or a combination thereof, should be applied to demonstrate that the structure, system or component will perform its safety function(s) to a level commensurate with its classification.		

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

5.8.2 ELECTRICAL, CONTROL AND INSTRUMENTATION STANDARDS

5.8.2.1 BS IEC 61226 (NPPs – I&C Important to Safety – Classification of I&C Functions) [Ref. 14] was produced in response to an IAEA requirement to classify NPP C&I systems and equipment according to their importance to nuclear 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;
- Assign specification and design requirements to C&I systems and equipment that performs the categorised functions.

5.8.2.2 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 discussed in this TAG.

5.8.2.3 BS IEC 61226 sets requirements for each safety function category relating to:

- The derivation of clear, comprehensive and unambiguous functional requirements through the 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;
  - Analysis (e.g. DBA, failure modes and effects analysis (FMEA)).
- The operating environment of the equipment delivering the safety function;
- Quality assurance through the lifecycle.

5.8.2.4 BS IEC 61513 (NPP – I&C Important to Safety – General Requirements for Systems) [Ref. 17] 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.

5.8.2.5 It should be noted that the current versions of both BS IEC 61226 and BS IEC 61513 relate to NPPs. 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-NPPs should be assessed using BS IEC 61508 (Functional Safety of Electrical / Electronic / Programmable Electronic Safety-Related Systems) [Ref. 19]. 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 TAGs:

- Safety Systems (NS-TAST-GD-003) [Ref. 3];
- Computer Based Safety Systems (NS-TAST-GD-046) [Ref. 20].

5.8.3 MECHANICAL ENGINEERING STANDARDS

5.8.3.1 Engineered SSCs should be designed to deliver their required safety functions with adequate reliability, according to the magnitude and frequency of the radiological hazard. This will 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;
- Asset management approach;
- Decommissioning.

5.8.3.2 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.

5.8.3.3 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.

5.8.3.4 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 required 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 safety tolerate) then seismic safety functions will need to be generated and categorised by the mechanical engineers to be placed on the civil engineering structures.

5.8.3.5 ONR assessors are expected to use judgment to determine if the licensee's / RP's arrangements are adequate to provide evidence that the level of substantiation for an SSC is commensurate with its classification.

5.8.3.6 Annex 2 of this TAG sets out mechanical engineering examples of design substantiation considerations and specific standards applicable for nuclear lifting equipment. However, the design phase approach outlined within Annex 2 is equally applicable to a range of mechanical SSC's. Further guidance to assist ONR assessors is set out in the following TAGs:

- Procurement of Nuclear Safety Related Items or Services (NS-TAST-GD-077) [Ref. 21];
- Design Safety Assurance (NS-TAST-GD-057) [Ref. 22];
- Licensee Design Authority Capability (NS-TAST-GD-079) [Ref. 23];
- Licensee Use of Contractors and Intelligent Customer Capabilities (NS-TAST-GD-049) [Ref. 24];
- Nuclear Lifting Operations (NS-TAST-GD-056) [Ref. 25];
- Asset Management (NS-TAST-GD-098) [Ref. 26].

5.8.4 STRUCTURAL INTEGRITY STANDARD – NUCLEAR PRESSURE EQUIPMENT DESIGN AND CONSTRUCTION

5.8.4.1 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.

5.8.4.2 Nuclear pressure vessel design and construction (PVDC) codes, such as ASME III [Ref. 27] and RCC-M [Ref. 28] 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.

5.8.4.3 UK experience of categorisation and classification of SSCs includes the categorisation of nuclear pressure equipment (NPE) for pressurised water reactors (PWRs). Previously NPE has been sub-divided into one of the three nuclear pressure vessel classes in accordance with ANSI N18.2 [Ref. 29]. 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. 30] 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. 31], 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.

5.8.4.4 Whilst UK experience to date is based on the approach used for Sizewell B it is not the only approach that can be used to determine the PVDC code class. Alternative approaches can be used to determine the PVDC code class. For example, the EPR™ 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.

5.8.4.5 In this example, the allocation of pressure vessel class is linked to the overall classification approach and defines a mechanical requirement level to set the nuclear pressure vessel design class and, where appropriate, the pressure vessel design code to ensure that the component quality is appropriate to fulfil the safety function it provides. Using this methodology there is the potential for Safety Class 1 and 2 components to be designed and manufactured to a lower level of Quality Assurance than would be expected from existing UK experience.

5.8.4.6 ONR places the emphasis is on the licensee / requesting party to justify the safety classification and PVDC code classification, and it may be beneficial to request a justification of any change from that of previous UK experience to ensure that an appropriate design and manufacturing standard is adopted for the given safety function.

5.8.4.7 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 RPV 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.

5.8.4.8 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 of the SAPs [Ref. 1], gives guidance on such situations and the level of demonstration required to make a highest reliability claim.

Engineering principles: integrity of metal components and structures: highest reliability components and structures	Safety case and assessment	EMC.1
The safety case should be especially robust and the corresponding assessment suitably demanding, in order that a properly informed engineering judgement can be made that: (a) the metal component or structure is as defect-free as possible; and (b) the metal component or structure is tolerant of defects.		

Engineering principles: integrity of metal components and structures: highest reliability components and structures	Use of scientific and technical issues	EMC.2
The safety case and its assessment should include a comprehensive examination of relevant scientific and technical issues, taking account of precedent when available.		

Engineering principles: integrity of metal components and structures: highest reliability components and structures	Evidence	EMC.3
Evidence should be provided to demonstrate that the necessary level of integrity has been achieved for the most demanding situations identified in the safety case.		

5.8.5 CIVIL ENGINEERING STANDARDS

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

5.8.5.2 For safety related civil engineering structures, 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 or claims.

5.8.5.3 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.

5.8.5.4 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.

5.8.5.5 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.

5.8.5.6 It is important to realise that it is not just the design standards that affect the reliability and hence ability of a civil engineering structure to deliver its safety functions. The fabrication and construction quality standards, and inspection and maintenance procedures applied during operation are also relevant.

6. REFERENCES

1. *Safety Assessment Principles for Nuclear Facilities*, ONR, Revision 0, November 2014, http://www.onr.org.uk/saps/index.htm;
2. *Licence Condition Handbook*, ONR, February 2017, http://www.onr.org.uk/silicon.pdf;
3. *Safety Systems*, ONR, NS-TAST-GD-003;
4. *Health and Safety at Work Act 1974*;
5. *Safety Related Systems and Instrumentation*, ONR, NS-TAST-GD-031;
6. *Limits and Conditions for Nuclear Safety (Operating Rules)*, ONR, NS-TAST-GD-035;
7. *Safety of Nuclear Power Plants: Design*, IAEA, Specific Safety Requirements No. SSR-2/1, Revision 1, February 2016;
8. *Safety Assessment for Facilities and Activities*, IAEA General Safety Requirements GSR Part 4 Revision 1;
9. *Safety of Nuclear Fuel Cycle Facilities*, IAEA, Specific Safety Requirements No. SSR-4, October 2017;
10. *Safety Classification of Structures, Systems and Components in Nuclear Power Plants*, IAEA, Specific Safety Guide No. SSG-30, May 2014;
11. *Application of the Safety Classification of Structures, Systems and Components in Nuclear Power Plant*, IAEA, IAEA-TECDOC-1787, April 2016;
12. *Report – WENRA Safety Reference Levels for Existing Reactors*, WENRA, September 2014;
13. *Report – Safety of New NPP Designs*, WENRA (Reactor Harmonisation Working Group), March 2013;
14. *BS EN IEC 61226: 2010 – Nuclear Power Plants – Instrumentation and Control Important to Safety – Classification of Instrumentation and Control Functions*;
15. *Human Reliability Assessment*, ONR, NS-TAST-GD-063;
16. *LC 22: Modification and Experimentation on Existing Plant*, ONR, NS-INSP-GD-022;
17. *BS EN IEC 61513:2013 – Nuclear Power Plants – Instrumentation and Control Important to Safety – General Requirements for Systems*;
18. *Probabilistic Safety Analysis*, ONR, NS-TAST-GD-030;
19. *BS EN IEC 61508:2010 – Functional Safety of Electrical / Electronic / Programmable Electronic Safety-Related Systems*;
20. *Computer Based Safety Systems*, ONR, NS-TAST-GD-046;
21. *Supply Chain Management Arrangements for the Procurement of Nuclear Safety Related Items or Services*, ONR, NS-TAST-GD-077;
22. *Design Safety Assurance*, ONR, NS-TAST-GD-057;
23. *License Design Authority Capability*, ONR, NS-TAST-GD-079;
24. *Licensee Core Safety and Intelligent Customer Capability*, ONR, NS-TAST-GD-049;
25. *Nuclear Lifting Operations*, ONR, NS-TAST-GD-056;
26. *Asset Management*, ONR, NS-TAST-GD-098;

27. *ASME Boiler and Pressure Vessel Code, Section III Rules for Construction of Nuclear Facility Components*, American Society of Mechanical Engineers (ASME), 2017 Edition;

28. *RCC-M, design and Construction Rules for Mechanical Components of PWR Nuclear Islands*, Published by the French Association for Design, Construction and In-Service inspection Rules for Nuclear Island Components, AFCEN 2007 Edition;

29. *Nuclear Safety Criteria for the Design of Stationary pressurised Water Reactor Plants*, American Nuclear Society Standards, ANSI N18.2 – 1, 1973;

30. *Nuclear Safety Criteria for the Design of Stationary pressurised Water Reactor Plants – American Nuclear Society Standards*, ANSI N51.1 – 1, 1983;

31. *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*, US NRC, March 2007.

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, inspection, 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
HSWA	Health and safety at work act
IAEA	International Atomic Energy Agency
I&C	Instrumentation and control
LC	Licence condition
NDT	Non-destructive testing
NPE	Nuclear pressure equipment
NPP	Nuclear power plant
NRC	Nuclear Regulatory Commission
ONR	Office for Nuclear Regulation
pfd	Probability of failure on demand
PSA	Probabilistic safety analysis
PVDC	Pressure vessel design and construction
PWR	Pressurised water reactor
R&D	Research and development
RGP	Relevant good practice
RP	Requesting party
RPV	Reactor pressure vessel
SAA	Severe accident analysis
SAP	Safety assessment principle

SFAIRP	So far as is reasonably practicable
SFR	Safety functional requirement
SMDC	Safety mechanism, devices and circuits
SSC	Structures, systems and components
TAG	Technical assessment guide
WENRA	Western European Nuclear Regulators' Association

8. ANNEX 1 – EXAMPLES

8.1 BASIS FOR EXAMPLES

8.1.1 The following examples provide some insights into how safety function categorisation and SSC classification may be reasonably applied. The categorisation and classification processes from sections 5.6 and 5.7 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 assessor understand the issues explored within this TAG.

8.2 EXAMPLE 1 – 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. It considers 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. This 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 Supposing the first function is not maintained, then some limited source corrosion could occur over a period of time. A small dose may result if an operator inhaled or ingested some of the contaminated water. Given these consequences, the first safety function could turn out to be Category C. If the loss of the shielding water could quickly lead to a fatal radiation dose to an operator, then the second function is likely to be Category A.

8.2.4 The identification and categorisation of the two distinct safety functions undertaken by the water treatment system is limited. So, 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 So, 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 EXAMPLE 2 – 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. Therefore the function has been designated as Category A. 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 An additional, diverse protective safety system also exists for the overheating fault consisting of a set of bursting discs, designed to relieve the build-up of pressure in the furnace due to excess heating. 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 may be to undertake a further breakdown in the original safety function. This identifies two separate sub-functions met by the two protective systems. In this approach, the Class 1 trip system addresses the first sub-function. However rather than considering the bursting discs as a second line of delivery of the overarching safety function, they 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 framework.

8.3.6 The potential difficulty that assessors 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 5.7.4 and reference 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 EXAMPLE 3 – 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. So, 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 protections 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 EXAMPLE 4 – POWER REACTOR DECAY HEAT REMOVAL: PRACTICAL CLASSIFICATION OF MULTIPLE LINES OF PROTECTION

8.5.1 This example, following-on from the previous scenario, explores one of the aspects in which SSC classification could be adjusted based on the engineering practicalities of fault protection.

8.5.2 Consider the removal of decay heat in a PWR following a fault affecting a normal operation system prompting a reactor trip. As the consequences for a fault on a PWR are likely to be severe and the fault may occur relatively frequently, let us suppose that the safety function of 'decay heat removal following reactor trip' 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 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 (e.g. for a reactor reliant upon active safety systems only), it would be expected that 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 may be acceptable to reverse this classification.

8.6 EXAMPLE 5 – AIRTIGHT HOUSING CONNECTED TO THE VENTILATION SYSTEM SERVING A LABORATORY THAT HANDLES RADIOACTIVE MATERIAL: CATEGORISATION REFINEMENT

8.6.1 This example explores the importance of the refinement step in the categorisation of safety functions that are driven by the potential consequences for people on the licensed site.

8.6.2 Consider an air filter within an airtight housing connected to the ventilation system serving a laboratory on a nuclear licensed site that handles radioactive materials. Although the airborne contamination levels in the laboratory are controlled and monitored to ensure they are well within acceptable limits, over time some activity does build up in the air filter.

8.6.3 Let us imagine that a sudden failure of the containment boundary provided by the filter housing. Conservatively, let us assume that this has been assessed to lead to the immediate release of a substantial amount activity which is assumed to fall onto a laboratory worker standing below and resulting in a maximum inhaled dose of 3 mSv. There are no radiological consequences outside the laboratory as the room provides a secondary containment boundary.

8.6.4 The initial categorisation of the safety function upon the filter housing to provide containment would (using Figure 3b) be Category B which would typically lead to Class 2 being ascribed to the filter module itself. However, it is important to consider the refinement step in determining the safety function categorisation.

8.6.5 Let us assume that the laboratory has activity-in-air monitoring and evacuation arrangements; that the worker is highly trained, radiologically classified and monitored; and that the workers wear simple dust masks due to other non-radiological hazards. Whilst these mitigating items do not detract from the significance of the preventative safety function placed upon the filter module to not fail, they do provide additional defence-in-depth and risk reduction to a fault sequence with relatively low consequences. Given that the risk is to a single radiation-classified individual there may be a good argument to refine the categorisation of the safety function to Category C and derive a SSC classification for the filter housing of Class 3.

8.6.6 Now consider an alternative scenario in which, rather than being housed within the laboratory, the filter is located on the outside of the building. Let us imagine that failure of the module housing would still result inhaled dose, after some dispersal, of 2 mSv; but that this could now impact 100 individuals in the nearby canteen on the licensed site. There are no off-site consequences. The initial categorisation of the containment safety function is still Category B; however, in this scenario there are no significant additional mitigating measures and the 2 mSv uptake would affect a much larger number of people, many of whom are not radiation workers as they include catering, administrative and staff from the site. Despite the same initial categorisation, there is a good argument here to retain the Category B for the safety function and seek the higher reliability associated with the assignment of Class 2 for the filter module.

8.6.7 Consider further the scenario in which in the on-site dose was 100 mSv to 1,000 individuals. This would still attract an initial safety function categorisation of Category B (from Figure 3b); however, this is clearly a very significant radiation dose to a very large number of people. In this case it would be reasonable for the refinement step to seek to increase the categorisation to Category A and thus to seek Class 1 integrity from the filter housing. Please remember that this example is hypothetical and is focussed on the categorisation refinement step discussed in the TAG – there are other ONR SAPs, not to mention RGP that would strongly oppose a situation in which a single failure in a single containment boundary could lead to such serious consequences to such a large number of personnel.

9. ANNEX 2 – FURTHER GUIDANCE ON MECHANICAL SYSTEMS

9.1 Table 4 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)	1. Design process robustness; guidance set out in ONR TAG: Design Safety Assurance (NS-TAST-GD-057) [Ref. 22]. Including consideration of 'informed customer capabilities' for new build (comparable with intelligent customer capability); guidance set out in ONR TAG: Licensee Core Safety and Intelligent Customer Capabilities (NS-TAST-GD-049) [Ref. 24]. 2. Safety analysis; undertake appropriate deterministic and PSA. 3. Optioneering studies; to reduce risks to ALARP; example of activities include: design reviews, risk assessment and FMEA; hazard and operability (HAZOP) studies etc. 4. Research and development; undertake appropriate research and development (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. 7. Codes and standards; adoption of : a. Specific nuclear codes and standards, (e.g. ASME; NOG etc.); b. Specific in-house guidance and quality management excluded from specific nuclear codes and standards.	1. Design process robustness; guidance set out in ONR TAG: Design Safety Assurance (NS-TAST-GD-057). 2. Safety analysis; undertake appropriate deterministic and probabilistic safety analysis. 3. Optioneering studies; to reduce risks so far as is reasonably practicable (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 ONR TAG: Supply Chain Management Arrangements for the Procurement of Nuclear Safety Related Items or Services (NS-TAST-GD-077) [Ref. 21].

	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, guidance set out in ONR TAG: Asset Management (NS-TAST-GD-098) [Ref. 26]. 9. Procurement arrangements; guidance set out in ONR TAG: Supply Chain Management Arrangements for the Procurement of Nuclear Safety Related Items or Services (NS-TAST-GD-077) [Ref. 21].	
Detailed design / manufacture (SSC product design intent demonstration)	1. Design authority and intelligent customer presence during procurement; guidance set out in ONR TAGs: a. Licensee Design Authority Capability (NS-TAST-GD-079) [Ref. 23]; b. Licensee Core Safety and Intelligent Customer Capabilities (NS-TAST-GD-049) [Ref. 24]. 2. Detailed design reviews etc. to reduce risks to ALARP. 3. 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, guidance set out in ONR TAG: Asset Management (NS-TAST-GD-098) [Ref.26] 4. SSC tests; e.g.: a. Product factory acceptance tests; b. Demonstration of specific FOAK EIMT aspects. 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.	1. Life time quality records; examples include: a. Vendor drawings; b. Certificate of conformity; c. Declaration of incorporation; d. Operating and maintenance manual etc.

	6. Life time quality records; examples include: a. Drawings; b. Calculations and FMEA; c. Material traceability records; d. Material certifications including welding consumables; e. Welding, non-destructive testing (NDT) procedures and records; 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.	
Site installation commissioning (SSCs design intent demonstration)	1. EIMT demonstrations should confirm the design intent and the requirements of LC 21 – Commissioning: a. Installation acceptance tests; b. System tests; c. Safety tests; 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 : a. LC 21 – Commissioning; b. LC 20 – Modification to design of plant under construction".	1. EIMT demonstrations should confirm the design intent and the requirements of LC 21 – Commissioning: a. Installation acceptance tests; b. System tests; c. Safety tests; d. Active tests and early operations etc. 2. Life time quality records documentation as required by: a. LC 6 – Documents, records, authorities and certificate; b. LC 20 – Modification to design of plant under construction.
Operations (SSC design intent maintained demonstration)	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: a. Plant maintenance schedule; b. Commensurate EIMT, surveillance and condition monitoring regime etc.	1. Life time quality records documentation as required by: a. LC 25 – Operational records; b. LC 22 – 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:

	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: a. LC 22 – Modification or experiment on existing plant; b. LC 15 – Periodic review.	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.
Decommission-ing (SSCs design intent demonstration)	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.	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.

Table 4 – Guidance on classification of mechanical systems by design phase