|  |
| --- |
|  |
| ONR Technical Assessment Guide  Categorisation of safety functions and classification of structures, systems and components (SSCs) |



ONR Technical Assessment Guide (TAG)

Categorisation of safety functions and classification of structures, systems and components (SSCs)

**Head of Profession**: - Fault Analysis

**Authored by**: Fault Studies Inspector

**Approved by**: Fault Analysis Head of Profession

**Issue**: 2.1

**Published**: May 2025

**Next scheduled review**: May 2028

**Document reference**: NS-TAST-GD-094

**Record reference**: [ONRHH-822789359-19711](https://prodonrgov.sharepoint.com/sites/HOW2Hub/_layouts/15/DocIdRedir.aspx?ID=ONRHH-822789359-19711)

Revision commentary

|  |  |
| --- | --- |
| Issue | Description of update(s) |
| 2.1 | New TAG template implemented. Minor updates to references. Improvements to clarity and correction of typos. Removal of prescriptive language. Restructured to improve readability. Explicit inclusion of relevant WENRA SRLs. Improved alignment to latest version of the SAPs. Improved clarity of expectations related to refinement factor (d) in the example SSC classification scheme. Removal of discipline specific guidance. |

Contents

[1. Introduction 4](#_Toc198029739)

[2. Purpose and scope 5](#_Toc198029740)

[3. Relationship to licence and other relevant legislation 6](#_Toc198029741)

[4. Relationship to Safety Assessment Principles, WENRA Reference Levels, and IAEA Safety Standards and Guides 8](#_Toc198029742)

[5. Advice to inspectors 11](#_Toc198029743)

[References 38](#_Toc198029744)

[Glossary and abbreviations 40](#_Toc198029745)

[Appendix 1 – Examples 41](#_Toc198029746)

# Introduction

1. ONR has established its [Safety Assessment Principles](http://www.onr.org.uk/saps/saps2014.pdf) (SAPs) (Ref. [1]) which apply to the assessment by ONR specialist inspectors of safety cases for nuclear facilities that may be operated by potential licensees, existing licensees, or other dutyholders. The principles presented in the SAPs are supported by a suite of guides to further assist ONR’s inspectors in their technical assessment work in support of making regulatory judgements and decisions. This technical assessment guide (TAG) is one of these guides.
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 (refer to SAP EKP.3). The identification and categorisation of safety functions and the identification and classification of structures, systems and components (SSCs) and human actions are key activities that are required to support reasonable and balanced implementation of defence in depth.
3. Safety function categorisation is the process by which safety functions are categorised based on their significance with regard to safety (refer to SAP ECS.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.
4. Classification is the process by which SSCs and human actions are classified on the basis of their significance in delivering associated safety functions (refer to SAP ECS.2). The classification assigned to an 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 (refer to SAP ECS.3).
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 ONR’s expectation that the safety function categorisation and SSC classification process is not influenced by preconceived design solutions.

# Purpose and scope

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. ONR assessors should use this TAG to assess the licensee’s / RP’s safety function categorisation and SSC classification arrangements during early engagement, generic design assessment (GDA), the permissioning process for new build, periodic safety reviews, and plant modification projects.
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 an 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;
* Appendix 1 contains examples to illustrate the categorisation and classification process;

1. This guide is restricted to nuclear safety function categorisation and SSC classification. It does not address the categorisation of documents, maintenance, engineering changes / plant modification proposals.   
   However, it should be noted that such categorisation should be informed by the category of safety functions and classification of SSCs to which they relate.
2. Whist this guide is not intended to provide specific guidance on the classification of human actions required to deliver or support the delivery of safety functions, an analogous classification method, as that used for SSCs, should be applied. The guidance presented within this TAG is therefore also broadly applicable to the classification of human actions and administrative controls that are necessary for safety.

# Relationship to licence and other relevant legislation

## Relevant licence conditions

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 (refer to 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 to a level of confidence commensurate with the SSC classifications justified within the safety case.

## Overarching UK legislation

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.

# Relationship to Safety Assessment Principles, WENRA Reference Levels, and IAEA Safety Standards and Guides

## SAPs

1. SAP ECS.1 and SAP ECS.2 refer directly to safety function categorisation and SSC classification respectively. SAP ECS.3 covers the relationship between SSC classification and codes and standards. This TAG focuses on these principles, although a number of other SAPs, such as SAPs ECS.4-5 and key principle SAPs EKP.3-5, are also relevant.

## TAGs

1. The Safety Systems TAG (NS‑TAST‑GD‑003) (Ref. [3]), provides guidance on determination of the need for safety systems, and their design expectations. The Safety Related Systems and Instrumentation TAG (NS‑TAST-GD-031, Ref. [5]) provides guidance on design expectations for safety-related systems. Both of these are impacted by the classification of the safety system or safety related system.
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.

## IAEA safety standards

1. The International Atomic Energy Agency (IAEA) fundamental safety principles (Ref. [7]) include the expectation that safety measures are applied and optimised in facilities and activities that give rise to radiation risks.   
   The safety measures should provide the highest level of safety that can reasonably be achieved throughout the lifetime of the facility or activity, without unduly limiting its utilisation.
2. To ensure a design meets these fundamental principles, multiple IAEA guidance documents include the requirement that all items important to safety shall 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. [8]);
* Safety Assessment for Facilities and Activities (GSR Part 4) (Ref. [9]);
* Safety of Nuclear Fuel Cycle Facilities (SSR-4) (Ref. [10]).

1. Further relevant guidance is provided within:

* Safety Classification of SSC in NNPs (SSG-30) (Ref. [11]);
* Application of the Safety Classification of SSCs in Nuclear Power Plants (IAEA-TECDOC-1787) (Ref. [12]).

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

## WENRA reference levels

1. Western European Nuclear Regulators Association (WENRA) safety reference levels for existing reactors (Ref. [13]) have been considered during the development of this TAG. The WENRA reference levels are considered to be RGP for existing civil nuclear reactors, as stated in Section 4 of NS-TAST-GD-005 (Ref. [14]).
2. In particular, Issue G covers “*Safety Classification of Structures, Systems and Components*”, and G1. Objective states:

G1.1: “*All SSCs important to safety shall be identified and classified on the basis of their importance for safety.*”

1. G1.1 is captured in SAP ECS.2 (refer to Section 5.3.3).
2. G2.1 and G2.2 provide further detail regarding the expectations for the SCC classification process:

G2.1: “*The classification of SSCs shall be primarily based on deterministic methods, complemented where appropriate by probabilistic methods and engineering judgment.*”

G2.2: “*The classification shall identify for each safety class:*

* *The appropriate codes and standards in design, manufacturing, construction and inspection;*
* *Need for emergency power supply, qualification to environmental conditions;*
* *The availability or unavailability status of systems serving the safety functions to be considered in deterministic safety analysis;*
* *The applicable quality requirements”*

1. G2.1 is captured in SAPs para 165, and G2.2 is captured in SAP ECS.3 and paras 169 – 173 (appropriate codes and standards) and EQU.1 (qualification procedures).
2. G3.1 and G3.2 provide expectations linking the reliability of SSCs to their classification:

G3.1: “*SSCs important to safety shall be designed, constructed and maintained such that their quality and reliability is commensurate with their classification.*”

G3.2: “*The failure of a SSC in one safety class shall not cause the failure of other SSCs in a higher safety class. Auxiliary systems supporting equipment important to safety shall be classified accordingly.*”

1. G3.1 is captured in SAP ECS.3, and Section 5.3.6 of this TAG. G3.2 is captured in SAPs para 167 and 168.
2. Finally, G4.1 and G4.2 provide expectations for SSC qualification:

G4.1: “*The design of SSCs important to safety and the materials used 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.*”

G4.2: “*Qualification procedures shall be adopted to confirm that SSCs important to safety meet throughout their design operational lives the demands for performing their function, taking into account environmental conditions over the lifetime of the plant and when required in anticipated operational occurrences and accident conditions.*”

1. G4.1 and G4.2 are captured in SAP EQU.1 (qualification procedures).
2. In addition, the WENRA report on the safety of new NPP designs (Ref. [15]) sets expectations that safety features specifically designed for fulfilling safety functions required in postulated core melt accidents shall be safety classified.

## International safety standards

1. The guidance contained in this TAG is consistent with BS EN IEC 61226 (NPPs – Instrumentation, control and electrical power systems important to safety – Categorization of functions and classification of systems) (Ref. [16]). BS EN 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.

# Advice to inspectors

## General

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. The exercise should take into account all potential internal and external hazard conditions that can affect defence in depth and the safe operation of the plant/activity (Ref. [12]).
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 and associated operator actions delivering those safety functions;
* That the principle of defence in depth is applied (with suitable and sufficient prevention, protection and mitigation);
* That RGP is applied and risks are reduced to ALARP (which may require design improvements to achieve);
* That classification informs the entire lifecycle of activities associated with SSCs (and associated operator actions where applicable).

1. 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 – Safety functions and their categorisation
* Section 5.3 – Structures, systems and components and their classification
* Section 5.4 – The level to apply categorisation and classification;
* Section 5.5 – Design and lifecycle implications of SSC classification;
* Section 5.6 – Example safety function categorisation scheme;
* Section 5.7 – Example SSC classification scheme;

## Safety functions and their categorisation

### Definition and purpose of safety functions

1. A safety function is a specific purpose that must be accomplished for safety (Ref. [1]). This means preventing or mitigating the radiological consequences that could arise from a nuclear facility during normal operation, as a result of faults, or in the event of an accident. 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.
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 (refer to SAP EKP.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. | | |

1. Table 1 is taken from the SAPs 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 measures that could be implemented and should not be taken as absolute rules.

Table 1 - Objective of each level of protection and essential means of achieving them.

| **Level** | **Objective** | **Defence/Barrier** |
| --- | --- | --- |
| Level 1 | Prevention of abnormal operation and failures 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 releases of radioactive material | Emergency control and on- and off-site emergency response |

1. 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, (refer to Safety Systems TAG, Ref. [3]).
2. 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 protect against escalation 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).
3. Note that as level 5 measures typically represent emergency responses, they are dominated by non-engineered measures (such as emergency responders, 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 on demand; however, the ONR assessor may consider that the rigorous application of a categorisation and classification scheme not to be the best or only way to ensure this.
4. 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. Safety functions are also sometimes described based on their position within the hierarchy of defence in depth, (e.g. ‘duty’ or ‘preventative’ functions / ‘fault’ or ‘protective’ functions / ‘accident’ or ‘mitigation’ functions).

### Identification of safety functions

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.
2. The fundamental safety functions for a nuclear reactor (refer to paragraph 540 of the SAPs and SAP ERC.1) are:

* control of reactivity (including preventing re-criticality following an event);
* removal of heat from the core; and
* 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. | | |

1. For non-reactor facilities (refer to 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. | | |

1. 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.

1. 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. | | |

1. The safety function breakdown process should take into consideration normal operations throughout the lifecycle of the facility and fault or accident conditions.
2. The safety function breakdown should usually continue to at least the point at which the safety functions become clearly attributable to the SSCs and human actions that will be subject to classification. This is discussed further in Section 5.4 and explored in the examples in Appendix 1.

### Safety function categorisation

1. SAP ECS.1 outlines the main expectations of safety function 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. | | |

1. 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), (refer to paragraph 160 of the SAPs). However, it is also an expectation of the SAPs that probabilistic safety analysis (PSA) and severe accident analysis (SAA) should be undertaken to ensure that all relevant failure conditions and levels of defence in depth are taken into consideration.

|  |  |  |
| --- | --- | --- |
| **Fault analysis: general** | Design basis analysis, PSA and severe accident analysis | FA.1 |
| Fault analysis should be carried out comprising suitable and sufficient design basis analysis, PSA and severe accident analysis to demonstrate that risks are ALARP. | | |

1. 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 (refer to Ref. [11]));
* 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.

1. 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.

1. As noted in Section 5.2.1, the safety functions should be described separately to the 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.
2. An example categorisation scheme is given in Section 5.6.

## Structures, systems and components and their classification

### Safety systems and safety-related systems

1. The SAPs describe an SSC as an item important to safety within the facility design which provides a safety function. The safety function provided by the SSC may be direct or indirect, e.g. the SSC may be important to safety because it supports another SSC which provides a safety function.
2. These SSCs are sometimes sub-divided into two sub-groups:

* safety systems; that act in response to a fault to protect against a radiological consequence (but have no role in normal operations), and
* safety-related systems, an item important to safety that is not part of a safety system. Safety-related systems are therefore systems in place to perform an operational function but which also provide a safety benefit.

1. 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 the defence in depth concept.
2. Both safety systems and safety-related systems should be classified according to the significance of their contribution to the safety functions that they support.
3. 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]).

### Safety measures and human based safety claims

1. SAP ECS.2 (refer to paragraph 5.3.3.1) focuses on the application of classification to SSCs. However, paragraph 164 of the SAPs states that where safety functions are delivered or supported by human action, these human actions should be identified and classified. It notes that the methods for classification should be analogous to those used for classifying SSCs. This view is supported by SAP EHF.3, 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, (refer to the Human Reliability Analysis TAG (NS-TAST-GD-063, Ref. [17]) and Procedure Design and Administrative Controls TAG (NS-TAST-GD-060, Ref. [18]) 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. | | |

1. The term safety measure encompasses both the human actions and SSCs needed in the delivery of safety functions. A safety measure is defined in the SAPs 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 measures | EKP.5 |
| Safety measures should be identified to deliver the required safety function(s). | | |

1. 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. Note that EKP.5 also outlines the hierarchy of safety measures, in which passive or automatic safety measures are preferable to those requiring human actions.

### SSC classification

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. | | |

1. 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 Ref. [11]);
* 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.

1. In line with paragraph 165 of the SAPs, 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]](#footnote-2) 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.

1. 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 Appendix 1 provide further guidance.

### Prevention versus protection

1. The most effective way to maintain safety is to prevent abnormal events and incidents occurring. IAEA SSR-2/1 (Ref. [8]) 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.
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.
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. An alternative solution may be to provide further guidance on how principal, significant and other can be interpreted when classifying an SSC.

### Number and quality of safety systems

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.
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 such as SAP ERC.2 and SAP EDR.4 may be relevant.
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. | | |

1. 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. | | |

### SSC reliability

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 (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.

Table 2 - Relationship between SSC class and the failure frequency and probability of failure on demand (refer to Ref. [3])

|  |  |  |
| --- | --- | --- |
| **SSC Class** | **Failure frequency per year (ff)** | **Probability of failure on demand (pfd)** |
| Class 1 | 10-3 ≥ ff ≥ 10-5 | 10-3 ≥ pfd ≥ 10-5 |
| Class 2 | 10-2 ≥ ff ≥ 10-3 | 10-2 ≥ pfd ≥ 10-3 |
| Class 3 | 10-1 ≥ ff ≥ 10-2 | 10-1 ≥ pfd ≥ 10-2 |

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

## The level to apply categorisation and classification

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.
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, for all plant operating states, including accident conditions. 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.
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.
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. 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, such as those arising from internal and/or external hazards, 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.

1. 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.
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.
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, as noted above, combining preventative, protective and mitigative elements in a single classified combination should 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.
4. For the issues discussed above, the use of hazard analysis and 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. Some examples illustrating the typical approach to safety function breakdown and classification and the assignment and classification of SSCs are provided in Appendix 1.

## Design and lifecycle implications of SSC classification

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. | | |

1. It should be noted that as SSC classification is directly linked to reliability (refer to Section 5.3.6), it is also linked with the robustness of the engineering and the incorporation of high reliability design principles (such as redundancy, diversity and independence). It is also linked with 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. [19]).
2. Codes and standards should be preferably nuclear-specific, leading to a conservative design commensurate with the importance of the safety function(s) being delivered. The licensee may be able to justify the use of a non-nuclear specific code or standard, particularly for Class 3 SSCs, where there might not be an established nuclear code or standard or where this would be disproportionate in the circumstances. The licensee should nevertheless demonstrate that the code or standard used is adequate given the significance of the safety function(s) that could be impacted. When making a judgement on the adequacy of the adopted codes and standards, ONR inspectors should also consider RGP for similar SSCs at similar plants.
3. SAPs ECS.4 and ECS.5 provide further expectations for where no appropriate established codes or standards exist.
4. 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, including internal and external hazards both individually and in combination;
* States which may have arisen because of a beyond design basis event or the escalation of a design basis fault;
* Situations in which significant unintended relocations or releases of radioactive material have occurred and need to be managed.

1. 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. [20]):

* 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 (refer to 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 (refer to 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 (refer to Section 5.3);
* 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 (refer to 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. Safety classification should also inform arrangements for ageing management (refer to NS-TAST-GD-109, Ref. [21]). 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 and / or associated human actions;
* 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.

**Decommission**

**Safety function categorisation**

* Fault analysis
* Functional breakdown & categorisation

**SSC classification**

* Allocation of functions to SSCs
* SSC classification

**Realise Protected Plant**

* Design
* Specify
* Produce, fabricate, manufacture

**Implement SSCs**

* Install
* Commission
* Verify

**Implement safety functions**

* Validate functional requirements

**Operations**

* Operate
* EIMT
* Modify

*Functional acceptance criteria*

*Design acceptance criteria*

*Functional Requirements*

*Detailed functional requirements*

Refine functional definitions to clarify how higher-level functions will be performed (optioneering)

**Project definition**

* Concept
* Scope
* Definition
* Functional specification
* Safety strategy

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

## Example safety function categorisation scheme

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).

1. This section **outlines** a process that would meet the expectations of SAP ECS.1 (refer to Section 5.2.3). 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.**
2. The suggested scheme makes use of the three categories recommended in the SAPs at paragraph 160:

* 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.

1. Figure 2shows 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.

### Step 1 – initial categorisation

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:
2. The consequences should the safety function not be performed.
3. The likelihood with which a demand is placed upon the safety function.
4. 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), 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. 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 in which the function will be required (b2).

(c3) Role of the safety function in achieving a stable, safe state

(a1) Off-site unmitigated dose

(a3) PSA and SAA

(a4) Longer-term risk (clean-up)

(c) The extent to which the safety function is required, either directly or indirectly, to prevent, protect against or mitigate the consequences of initiating faults

**STEP 1**

**Initial safety function categorisation (refer to Figure 3)**

**STEP 2**

**Final safety function categorisation including other factors**

(a) The consequence of failing to deliver the safety function

(b) The likelihood that the safety function will be called upon

(c2) Impact on consequences for partial delivery of the safety function

(a2) On-site unmitigated dose

(c1) Role and position of the safety function in the hierarchy of defence in depth

(b1) For a safety function required during normal operation usually assume that there is a continuous demand upon the function

(b2) For a safety function following a fault or accident condition use total best estimate frequency of sequences calling upon the function

*To inform SSC classification*

*The factors from SAP ECS.1*

(a5) Nature of on-site doses

Figure 2 - Safety function categorisation scheme

1. 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 3) and one for the dose on site (a2 and Figure 4). 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.
2. For reference, the basic safety objective (BSO) and the basic safety level (BSL) from SAP Target 4 are included. The regions in Figure 3 and Figure 4 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.

10–3

10–4

10–5

Total frequency of demand on the safety function (/yr)

Off-site unmitigated and unprotected radiological consequences of failing to deliver the safety function (mSv)

0.01

1

10

100

Cat A

Cat B

Cat C

Target 4 BSL

Target 4 BSO

0.1

For information:

Indicative Regions for Initial Categorisation

Figure 3 - Off-site frequency / consequence regions for initial safety function categorisation (refer to Section 5.6.1)

10–3

10–4

Total frequency of demand on the safety function (/yr)

On-site unmitigated and unprotected radiological consequences of failing to deliver the safety function (mSv)

0.1

20

200

500

Cat A

Cat B

Cat C

Target 4 BSL

Target 4 BSO

2

Indicative Regions for Initial Categorisation

For Information:

10–5

Figure 4 - On-site frequency / consequence regions for initial safety function categorisation (refer to Section 5.6.1)

1. 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).

### Step 2 – refinement

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.
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.
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.
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 5.3.4.
5. Another factor is (c2) the potential reduction or exacerbation in consequences should there only be partial delivery of the safety function.
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 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 stable, safe 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.

## Example SSC classification scheme

1. This section outlines an SSC classification scheme satisfying the expectations of SAP ECS.2. It makes use of the three-class scheme recommended in the SAPs at paragraph 166:

* 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.

1. 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.
2. Figure 5 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.

**STEP 1**

**Initial SSC classification (refer to Table 2)**

**STEP 2**

**Final SSC classification including other factors**

(b) The probability that the item will be called upon to perform a safety function

(a) The category of safety function(s) to be performed by the item

(d) 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

*from safety function categorisation*

*To inform the application of the appropriate standards in the design, manufacture, construction, installation, commissioning, quality assurance, maintenance, testing and inspection and operation of the SSC (SAP ECS.3)*

(e) Reliability requirements derived to achieve an ALARP position with respect to PSA, DBA, SAA and SAPs Numerical Targets 4-9 (PSA and SAA, Ref. [1])

*The factors from SAP ECS.2*

(b1) Prominence of the SSC in the delivery of the safety function:  
● principal means;  
● significant means;  
● other means.

(c) The potential for failure to initiate a fault or exacerbate the consequences of an existing fault, including situations where the failure affects the performance of another SSC

Figure 5 - SSC classification scheme

### Step 1 – initial classification

1. The first step assigns an initial expectation of the SSC classification using Table 3. 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[[2]](#footnote-3). 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, (refer to Section 5.3.4 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.

1. 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 (Ref. [3]), any SSCs assigned to a backup measure may then step-down to the next lower class in line with the table. If two means of providing a safety function are identified, then one of them should be identified as the principal means. It is not normally appropriate to identify both systems merely as significant means, as this may evade the higher classification associated with the principal means of delivering the particular category of safety function.

Table 3 - Initial SSC classification

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

1. 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.
2. It is ONR’s expectation that the combinations of categorisation and classification, presented in Table 3, 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. Deviations from this would be expected to be supported by a robust justification that the approach adopted reduces risks to ALARP.
3. 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 Figure 3 and Figure 4). 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.

### Step 2 – refinement

1. The second step of classification incorporates a number of remaining aspects, as shown in Figure 5. 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.
2. One factor is (c) the potential for the SSC itself to initiate a fault or exacerbate the consequences of an existing fault, including by initiation of internal hazards, or as a consequence of its failure in the event of an external hazard. 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.
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 (refer to Section 5.6.2), and therefore should not be double counted if refinement has already been incorporated in the categorisation process. 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.
4. It would not typically be appropriate, without further justification, to apply an arbitrary fixed time within the classification scheme, following which the classification of SSCs can be reduced. Instead, refinement of classification based upon the time following the initiating fault at which the SSC is required, should be linked to a justifiable decrease in the importance of that SSC in the delivery of its assigned safety function. For example, this factor may be credited if grace times following the failure of an SSC provided to establish the stable, safe state (distinct from those provided for reaching the controlled state), would be demonstrably sufficient to restore the necessary safety functions, before any escalation of consequences. This would normally be expected to be demonstrated on a case-by-case basis.
5. 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. 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.
6. The link between reliability and class of the SSC is discussed in Section 5.3.6.
7. Both PSA and hazard analysis are 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. | | |

|  |  |  |
| --- | --- | --- |
| **Engineering principles: external and internal hazards** | Analysis | EHA.6 |
| The effects of internal and external hazards that could affect the safety of the facility should be analysed. The analysis should take into account hazard combinations, simultaneous effects, common cause failures, defence in depth and consequential effects. | | |

1. 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 the use of PSA is contained in the ‘*Use of PSA and probabilistic insights*’ TAG (NS-TAST-GD-116, Ref. [22]).

# References

|  |  |
| --- | --- |
| [1] | ONR, “Safety Assessment Principles (SAPs) for Nuclear Facilities,” 2014 Edition, Revision 1, January 2020. |
| [2] | ONR, “Licence condition handbook,” February 2017. [Online]. Available: https://www.onr.org.uk/media/gixbe2br/licence-condition-handbook.pdf. |
| [3] | ONR, “Safety Systems,” NS-TAST-GD-003, Issue 9.2, November 2022. |
| [4] | Health and Safety at Work etc. Act 1974. |
| [5] | ONR, “Safety Related Systems and Instrumentation,” NS-TAST-GD-031, Issue 7, May 2023. |
| [6] | ONR, “Limits and Conditions for Nuclear Safety (Operating Rules),” NS-TAST-GD-035, Issue 7, March 2023. |
| [7] | IAEA, “Fundamental Safety Principles,” SF-1, 2006. |
| [8] | IAEA, “Safety of Nuclear Power Plants: Design,” SSR-2/1 (Rev. 1), 2016. |
| [9] | IAEA, “Safety Assessment for Facilities and Activities,” GSR Part 4 (Rev. 1), 2016. |
| [10] | IAEA, “Safety of Nuclear Fuel Cycle Facilities,” SSR-4, 2017. |
| [11] | IAEA, “Safety Classification of Structures, Systems and Components in Nuclear Power Plants,” SSG-30, 2014. |
| [12] | IAEA, “Application of the Safety Classification of Structures, Systems and Components in Nuclear Power Plants,” IAEA-TECDOC-1787, 2016. |
| [13] | WENRA, “WENRA Safety Reference Levels for Existing Reactors 2020,” February 2021. |
| [14] | ONR, “Regulating duties to reduce risks to ALARP,” NS-TAST-GD-005, Issue 12.1, September 2024. |
| [15] | WENRA, “Safety of new NPP designs,” March 2013. |
| [16] | BS EN IEC 61226: 2021, “Nuclear power plants - Instrumentation, control and electrical power systems important to safety - Categorization of functions and classification of systems,” July 2021. |
| [17] | ONR, “Human Reliability Analysis,” NS-TAST-GD-063, Issue 6, December 2022. |
| [18] | ONR, “Procedure Design and Administrative Controls,” NS-TAST-GD-060, Issue 5, December 2022. |
| [19] | ONR, “LC 22: Modification or Experiment on Existing Plant,” NS-INSP-GD-022, Issue 7, January 2022. |
| [20] | BS EN IEC 61513:2013, “Nuclear power plants - Instrumentation and control important to safety - General requirements for systems,” March 2013. |
| [21] | ONR, “Ageing and Degradation Management TAG,” NS-TAST-GD-109, Issue 1, February 2023. |
| [22] | ONR, “Use of probabilistic safety analysis (PSA) and probabilistic insights,” NS-TAST-GD-116, Issue 1, September 2024. |
| [23] | IAEA, “IAEA Nuclear Safety and Security Glossary,” 2022. |

# 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

# Appendix 1 – Examples

## Basis for examples

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.
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.

## Example 1 – Radioisotope shielding tank water filter system: safety function breakdown and level of classification

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.
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.

1. 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.
2. 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.
3. 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.

## Example 2 – Electrically-powered furnace: classifying systems and the treatment of protection versus mitigation

1. This example explores the approaches and potential pitfalls associated with identifying and classifying protective and mitigative safety systems.
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.
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.
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.
5. Now consider that there are additional safety systems that are able to mitigate the radiological consequences. In this example, for instance, there 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.
6. The potential difficulty that assessors should look for in this example is where the protective (over-temperature trip and bursting discs) 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 pitfall occurs if it is argued that the overall Class 1 standard can be built-up from lower standards in each of the different items.
7. This approach should be viewed with caution (refer to Section 5.3.4 and Ref. [3]). It could be avoided by ensuring a sufficiently detailed safety function breakdown and the classification of the clearly distinct safety systems as separate entities rather than as an agglomeration. Classifying combinations of systems should be limited to those situations in which the systems involved have features that might make them susceptible to common-cause failure.

## Example 3 – Very low power assembly reactivity control: prevention versus protection and appropriate classification

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.
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.
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.
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.
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.
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.

## Example 4 – Power reactor decay heat removal: practical classification of multiple lines of protection

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.
2. Consider the removal of decay heat in a PWR following a fault affecting a normal operation system prompting a reactor trip. As the unmitigated consequences for a fault on a PWR could 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.
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, 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.
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.
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.

## Example 5 – Airtight housing connected to the ventilation system serving a laboratory that handles radioactive material: categorisation refinement

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.
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.
3. Let us imagine 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 of activity which is assumed to fall onto a laboratory worker standing below and resulting in a maximum inhalation dose of 3 mSv. There are no radiological consequences outside the laboratory as the room provides a secondary containment boundary.
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.
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, and assuming there are many conservatisms in the analysis predicting a dose close to the 2 mSv boundary, it may be grossly disproportionate to expect a Category B, Class 2 and an ALARP argument could potentially be made to refine the categorisation of the safety function to Category C and derive an SSC classification for the filter housing of Class 3.
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 in an inhalation 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 and administrative staff from the site. Despite the same initial categorisation, there is a good argument here to retain Category B for the safety function and seek the higher reliability associated with the assignment of Class 2 for the filter module.
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.

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. [↑](#footnote-ref-2)
2. 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. [↑](#footnote-ref-3)