CATEGORISATION AND CLASSIFICATION

Categorisation of Safety Functions

Once the significant faults and hazards have been identified the key safety functions can be determined to ensure that the plant design will be adequate to support safe construction, commissioning, operation, maintenance and decommissioning. The output of the analysis of commercial operations, and the initial fault and hazard identification activities is used to inform the development of the safety functions and their categorisation and classification.

The output of the analysis of commercial operations, and the initial fault and hazard identification activities is used to inform the development of the safety functions. The purpose of safety functions is to provide a clear and concise statement of the safety requirements that must be met by the plant or system in question. There is no single correct format for presenting safety functions. However, safety functions should relate to the prevention of an undesirable consequence from an identified hazard challenge. A suggested format for presenting Fundamental Safety Functions (*FSF*) is shown below:

- **FSF1**: Control of Reactivity – Prevent radiological consequences to workers and the public as a result of loss of reactivity control.

FSFs form the top level of a hierarchical safety function structure and are not related to specific safety measures. To provide the link to the specific safety, functional and performance requirements on the individual safety measures claimed to deliver each FSF, it is necessary to deconstruct them into High-Level Safety Functions (*HLSFs*). HLSFs should be provided with unique identifiers that link them to the corresponding FSFs. The following are examples of HLSFs relating to the control of reactivity:

- **HLSF 1-1**: Functions to prevent excessive reactivity insertion.
- **HLSF 1-2**: Functions to prevent changes in core geometry.
- **HLSF 1-3**: Emergency shutdown of the reactor.

All safety functions associated with a facility or activity shall be identified, assessed and categorised according to their safety significance, and the assessed Structures, Systems and Components (*SSCs*) significant to safety shall be correspondingly classified.

The Fundamental Nuclear Safety Principles (*FNSP*) should define the basis for the categorisation of safety functions. An example is given below:

- **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.

There is no simple definition of **principal** and **significant** and the interpretation of the above into a usable categorisation process therefore requires further guidance. The method for categorising safety functions 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 function is required, either directly or indirectly, to prevent, protect against or mitigate the consequences of initiating events.

An example categorisation scheme is shown in Figure 1 for both on-site and off-site consequences.

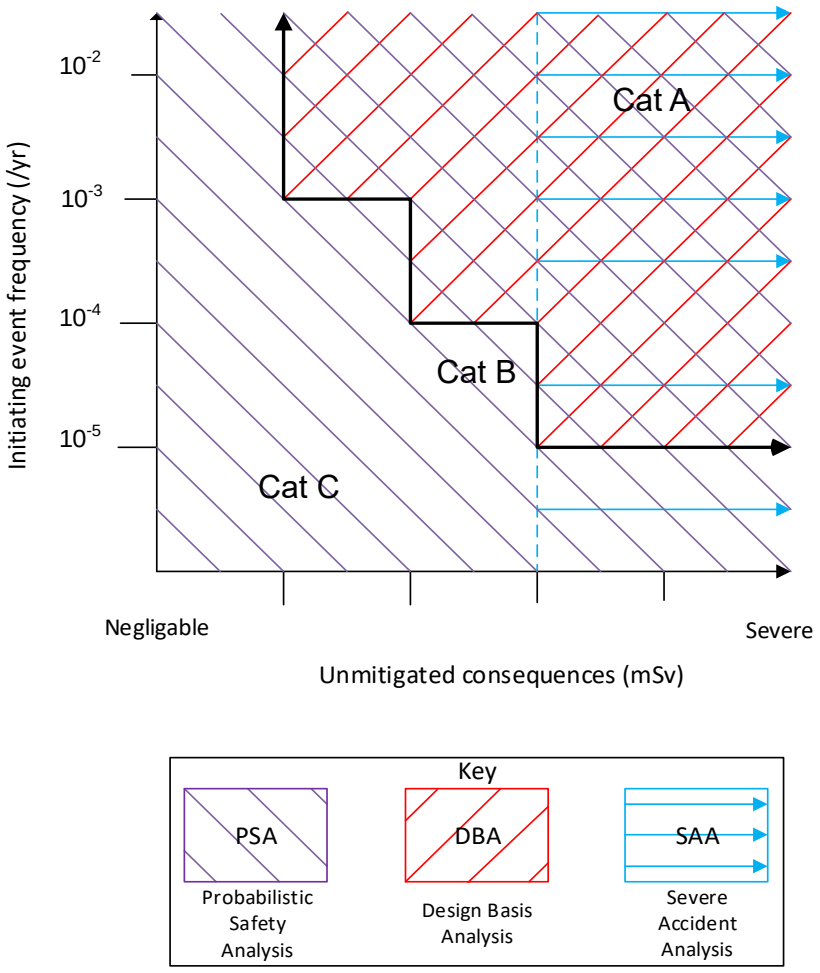

Figure 1: Event categorisation scheme.

The categories can be further described as follows:

- **Category A**: safety functions which play a principal role in ensuring nuclear safety, in that they are associated with the removal of intolerable radiological risks from design basis faults by either prevention of the risks or reduction of the risks to broadly acceptable levels.
- **Category B**: safety functions which make a significant contribution to nuclear safety, in that they are associated with the removal of radiological risks outside the design basis region either preventing

the risks or reducing the risks to broadly acceptable levels for foreseeable events and beyond design basis accidents, which are identified in fault studies.

- **Category C**: safety functions that do not fall into Category A or B safety functions or identified from As Low As Reasonably Practicable *(ALARP)* analyses as a reasonable additional function to implement.

Classification of Structures, Systems and Components

Once the initiating faults / events have been identified, and the unmitigated consequences and best estimate frequencies assessed, it is necessary to identify suitable and sufficient safety measures to ensure that the safety functions are derived.

Once candidate safety measures have been identified SSCs are classified on the basis of their safety significance to allow their integrity requirements to be defined. The classification scheme applied should take account of the category of the safety function being delivered by the SSC, the likelihood that the SSC will be required to perform its safety function, the potential for failure of the SSC to initiate a fault or impact another SSCs ability to deliver its safety function, and the time period in which the SSC is required to deliver its safety function.

When specifying safety measures the following hierarchy should be applied:

- Passive safety measures.
- Automatically initiated active engineered systems.
- Manually initiated active engineered systems.
- Administrative controls.
- Mitigation measures.

This hierarchy includes measures which are delivered or supported by human action. Although human actions are not classified using the same scheme as SSCs, it may be appreciated that all human-based safety claims should also take into account the category of the safety function being delivered / supported.

The FNSPs should define the basis of a classification scheme, an example of which is given below:

- **Class 1**: SSCs claimed as being the principal or first line means of delivering a Category A safety function; generally referred to as A1.
- **Class 2**: SSCs claimed as being the second line or diverse means of delivering a Category A safety function or the principal or first line means of delivering a Category B safety function and referred to as A2 and B2 respectively.
- **Class 3**: SSCs claimed as being a third line means of delivering a Category A safety function, a second line means of delivering a Category B safety function or delivering a Category C safety function referred to as A3, B3 and C3 respectively.

An example classification scheme formed by combining the category and classification definitions is provided in Table 1.

Safety Function Category	SSC Classification		
	Class 1 SSCs	Class 2 SSCs	Class 3 SSCs
Category A Protection for Design Basis (*DB*) Faults	Principal or first line delivery	Secondary delivery	ALARP
Category B Protection for Beyond Design Basis (*BDB*) Faults Protection for Foreseeable Events		Principal or first line delivery	Secondary delivery or ALARP
Category C Other Safety Functions			Secondary delivery or ALARP

Table 1: Example classification scheme.

For frequent DB faults (>10-3 /y) two lines of protection are required to deliver the fundamental safety functions. The SSCs claimed as the principal means of delivering each safety function are Class 1 and those claimed as the secondary or diverse means are at least Class 2.

Note: failure of the first line of defence (A1) is not entered as a new fault in the fault schedule. This gives clarity to the fact that the A2 system provides a significant contribution to satisfying the safety function derived from the original initiating event. It is therefore not considered as a new initiating event with the A2 system as a new principal means of providing the safety function.

Additional Information & Guidance

- http://www.onr.org.uk/resources.htm