A REVIEWED APPROACH TO SAFETY CLASSIFICATION OF SSC IN NUCLEAR REACTORS

N. A. MASRIERA, A.S. DOVAL, J.A. WEIGANDT
INVAP, Nuclear Business Division
Av. Cmte. Luis Piedrabuena 4950 R8403CPV Bariloche, Rio Negro - Argentina

In the frame of activities reinforcing Nuclear Safety Culture, within INVAP's activities on Knowledge Management, several critical areas of specialised knowledge were reviewed and developed into modules for training and discussion. When reviewing the subject of Methodology of Safety Classification of Structures, Systems and Components (SSC), a space for improvement was identified and the overall approach was re-developed keeping consistency with the safety classification concepts of the best practices and with IAEA guidelines.

The proposed structured method for performing safety classification is a top down process that begins with a basic understanding of the plant design at a functional level and its safety assessments, and allows assigning a safety class to every SSC essentially by the significance of its postulated failure.

The main improvements are related to including in the methodology all the SSC required to fulfil the safety functions (not only on the reactor), and to the ordering of these functions in a systematic way. SSCs are ordered in "types" based on their role in safety assessments (essentially safety analysis and radiological assessments). Mainly these types are: SSC performing Fundamental Safety Functions (FSF) on the reactor, SSCs relevant on Radiological Protection over other radioactive inventories, SSCs providing safety relevant information to operators and SSCs producing the conditions for the equipment and operators to work.

Clear identification of SSC types is essential to a safety classification process. The safety concept of Defence in Depth (DiD) is particularly relevant for the safety assessment of SSCs performing active functions on the reactor, as it sets "rules" for the assessments and for the categorisation of the functions performed at different DiD levels. Other SSCs are classified without assigning a category to their function.

The outcome of the safety classification process (Safety Class of each SSC) is used as an input to define the Safety Requirements (i.e. functional and engineering requirements to be compiled in a Licensing Basis), the Quality Level and the Seismic Class of each SSC.

The development of this methodology as presented in this work, capitalised the valuable experience gained in Research Reactors projects (e.g. PALLAS) with INVAP as a Nuclear Vendor, in activities of INVAP as a TSO over domestic reactors projects (e.g. CAREM SMR), and in individual expertise.

1. Introduction

The statement from IAEA SSG-30, reference [1] is endorsed: "*The goal of safety classification is to identify and classify those SSC that are needed to protect people and the environment from harmful effects of ionizing radiation, based on their roles in preventing accidents, or limiting the radiological consequences of accidents should they occur*."

This document provides a structured method for performing safety classification of SSC important to safety based on their functions and safety significance, assigning three safety classes with Safety Class 1 (SC 1) to the most safety relevant. This methodology is consistent with the concepts of safety classification set out in IAEA standards [1] and [2], developing further the use of the Defence in Depth (DiD) safety concept and the scope covering systems beyond the ones performing the Fundamental Safety Functions on the nuclear reactor.

The methodology presented is applicable to the SSCs of a Nuclear Reactor of OPAL type, i.e. an open pool reactor, with facilities for irradiation, testing and production.

Safety classification is a top down process that begins with a basic understanding of the plant design at a functional level, its safety assessments (essentially safety analysis and radiological assessments) on how the safety functions will be achieved. The SSC of the design required to fulfil the safety functions are systematically identified, and then ordered in "types".
The safety concept of DiD is relevant for the deterministic safety assessment of systems performing FSFs on the reactor and on materials that are being irradiated in or near the reactor core and participate in the dynamics of the nuclear reaction.
SSC not performing functions within the DiD concept are also classified. For example, an SSC identified as Passive Provisions does not perform within DiD, and is assigned a Safety Class directly: the significance of the SSC postulated failure fully defines its safety class without the need of categorizing the associated safety function, in line with reference [1].
The outcome of the safety classification process (the Safety Class of each SSC) is used as an input to define Safety Requirements (i.e. Safety Design Basis, or functional and engineering requirements relevant on safety), the Quality Level and the Seismic Class of each SSC.

2. Safety Classification Process

2.1. Overall description of the process

The overall safety classification process consists of the following main steps:

a) General understanding of the plant design, by its safety assessments, considering operating conditions and also credible accidental scenarios to be considered in the design process by how the safety functions will be achieved.
b) Identification and ordering of safety functions, described in section 2.2
c) Identification of SSC by type, described in section 2.3
d) Categorization of the Safety Functions, described in section 2.4
e) Preliminary safety classification of SSC, described in section 2.5
f) Guidelines for class reduction, described in section 2.6
g) Specific aspects of Safety Classification of SSC, described in section 2.7

In line with international practices, the methodology makes use of three Safety Categories for functions and three Safety Classes for SSCs. The functions derived from the FSFs are categorized based on their insertion in the DiD scheme, using three different factors.
The next step in the process is to identify the SSCs by types, and then to assign the preliminary safety class to all SSCs important to safety. For SSCs performing safety functions on the reactor, within DiD concept (SSCs type A), the preliminary Safety Class is given by the Safety Category of the Safety Function they perform. The preliminary classification defines the safety class of all the (other) types of SSCs (not performing within DiD levels) without assigning a category of the associated safety function. A Safety Class is not assigned to SSCs that do not fulfil any safety function and they are designated as "NA" (Not Applicable).
Figure 1 shows an overall schematic flow chart for the safety classification process, covering in the left column the case of SSCs type A and the right column the case for the rest of types of SSCs, reaching both the assignation of a preliminary Safety Class. In the figure it is clearly shown that safety categorization is only performed for type A SSCs. The process for assigning a final Safety Class and beyond is common for all type of SSC.
The following sections present further details of each one of the steps of these schemes.

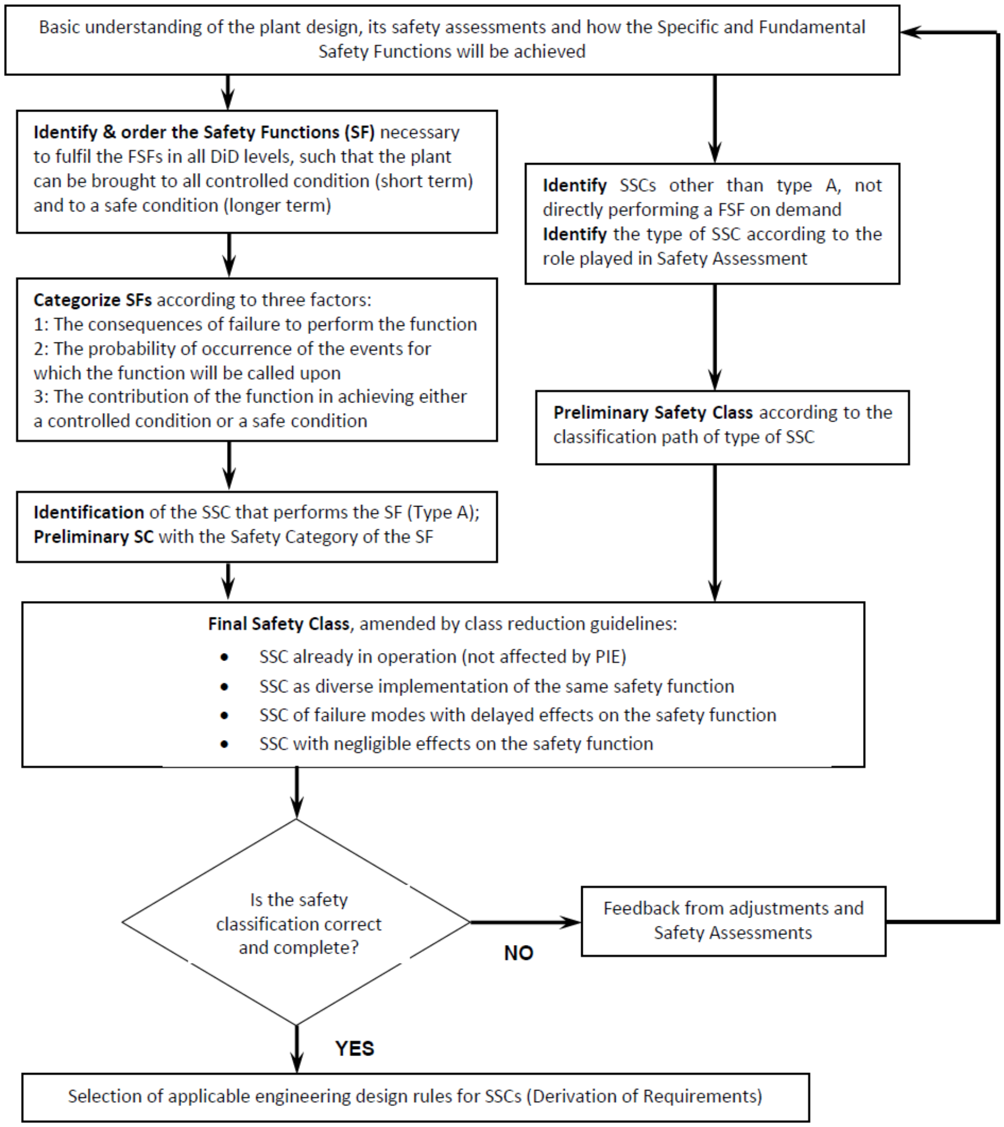

Figure 1: Simplified flow-chart of the safety classification procedure

2.2. Identification and ordering of safety functions

This section describes the identification and ordering of two sets of functions relevant on nuclear or radiological safety, namely Safety Functions and Specific Safety Functions.

The safety assessments (safety analysis and radiological assessments) are essentially procedures of deterministic functional analysis of the plant design. The safety functions assessed are:

a) **Safety Functions**, required to actively perform the Fundamental Safety Functions, credited in the deterministic Safety Analysis, demanded in a specific DiD level.

b) **Specific Safety Functions**, considered in the safety analyses and radiological assessments without taking part of the DiD scheme of levels, including:

- Confinement – radioprotection functions on radiological inventories other than the core;
- Functions that are performed regardless the occurrence of PIEs and triggered sequences;
- Monitoring functions providing the plant staff information to diagnose the situation;
- Support and auxiliary functions.

2.2.1. Identification of Safety Functions

The SSCs perform the FSFs in different ways for the different reactor operational states of normal operation, and the connection between SSC and DiD levels might differ. During Basic Design Stage the identification and ordering of the safety functions and the safety classification of SSCs are usually performed considering conditions connected to normal operation in the Power State. Safety Functions are presented in the following tables.

Table I: Safety Functions defined for performing the FSFs on demand by SSCs of the reactor

SF Name	Safety Function Description	DiD Level	Safety Categ	FSF
C1	**Trigger** actions to shut down the reactor and the PCS pumps in **DBA**.	3a	1	r, k
C2	**Trigger** actions to shut down the reactor and the PCS pumps in **DEC**.	3b	2	r, k
C3	**Control** the reactor core **reactivity** regulation in **AOO**.	2	2	r
C4	**Control** the reactor core **reactivity** regulation in **NO**.	1	3	r
C5	**Control** the reactor core and fissile targets **heat removal** during **NO and AOO**	1, 2	2	k
C6	**Control** the **confinement** in case of **DEC and Postulated Core Damage Accident**	3b, 4	2	b
R1	**Shut down** the reactor in case of **DBA**	3a	1	r
R2	**Shut down** the reactor in case of **DEC**	3b	2	r
R3	**Regulate** the reactor core **reactivity** during **NO and AOO**	1, 2	2	r
KC1	**Remove decay heat** from the **core** in case of **DBA and DEC**	3a, 3b	1	k
KC2	**Remove heat** from the **core** during **NO and AOO**	1, 2	2	k
KT1	**Remove decay heat** from the **fissile targets** in case of **DBA and DEC**	3a, 3b	1	k
KT2	**Remove heat** from the **fissile targets** during **NO and AOO**	1, 2	2	k
KW1	**Keep coolant** inventory for the reactor core and fissile targets in **DBA**	3a	1	k
KW2	**Keep coolant** inventory for the reactor core and fissile targets in **DEC**	3b	2	k
KW3	**Keep coolant** inventory for the reactor core and fissile targets in **NO and AOO**	1, 2	2	k
KWL1	**Keep coolant** inventory for the reactor core and fissile targets in the **long term**	3a, 3b	2	k
KL1	**Transfer heat to the Ultimate Heat Sink (UHS)** from the reactor **core** and fissile **targets** in the **long term** in case of **DBA and DEC**	3a, 3b	2	k
KL2	**Transfer heat to the UHS** from the reactor **core** and fissile **targets** in **AOO, long term**	2	2	k
KCL3	**Transfer heat to the UHS** from the reactor **core** during **NO**	1	3	k
KTL3	**Transfer heat to the UHS** from **fissile targets** during **NO**	1	3	k
B	**Confine** radioactive material coming from **core** or fissile **targets** damage	4	2	b

Table II: Safety Functions ordering table

DiD level (Plant State)	**Fundamental Safety Functions**							
	Reactivity		**Heat removal and transfer**				**Confinement**	
	Control by I&C system	By Reactivity management system	Water inventory	Heat removal/transfer to short-term UHS		Heat transfer to Long-term UHS	Barriers	Retention
				Core	Fissile Target			
DiD 1 (NO)	C4, C5	R3	KW3	KC2	KT2	KCL3, KTL3	(*1)	
DiD 2 (AOO)	C3, C5	R3	KW3	KC2	KT2	KL2	(*1)	
DiD 3a (DBA)	C1	R1	KW1, KWL1	KC1	KT1	KL1	(*1)	
DiD 3b (DEC with **no** core damage)	C2	R2	KW2, KWL1	KC1	KT1	KL1	(*1)	
DiD 4 (CDA/DEC with core damage)	C6	(*3)	(*3)	(*3)	(*3)	(*3)	(*2)	B

Notes (*1): by Passive Provisions Primary Barrier – cladding
(*2): by Primary Barrier – fuel cladding, by Reactor Containment in extended Loss Of Electric Power
(*3): these safety functions are performed by systems operated manually in scenarios DiD 4

Table 1 is an example of a list of the identified Safety Functions that are required to achieve each of the FSF where, the letter “r” indicates the FSF of reactivity control, “k” cooling and “b” confinement of radioactive materials, unfolded according to the DiD level in which the function is demanded, mentioning the safety category that is later explained.

The ordering of the identified Safety Functions necessary to fulfil the FSFs in all DiD levels is presented in Table II, allowing to verify the completeness of the list of Table I.

2.2.2. Specific Safety Functions

The functions considered in the safety analysis and radiological assessments without taking part of the DiD scheme of levels are addressed in the design of the reactor as Specific Safety Functions (SSF), as a way to distinguish them from the Safety Functions of Table I. Table III will present the preliminary list of the Specific Safety Functions of a reactor SSCs.

The main goal of producing a list of SSFs is to provide a set of names and descriptions that can be referenced or quoted in other sections and chapters of the Safety Analysis Report and in engineering documents. The names of the SSCs considered are the ones of a specific design: a Nuclear Reactor of OPAL type.

2.3. Identification of the type of SSC

SSCs that fulfil a safety function are safety relevant, and are identified in different types according to the role they play in the safety demonstration process. These types are:

a) **Type A: Reactor Systems** actively perform a FSF within the DiD safety concept, applied to a “reactor” including the core and materials being irradiated in or near the core taking part of the dynamics of the nuclear reaction. This type of SSC includes the systems actively performing a FSF in Normal Operation (DiD 1), such as the Primary Cooling System or the Automatic Power Regulation System (automatic pilot).

b) **Type B: Retention Systems** actively fulfil a function of confinement of radioactive material, other than the “reactor” (see previous paragraph), i.e. SSFs related to active retention in water or air, by ventilation and purification systems, by providing to these systems and by actively preventing the failure of confinement barriers.

c) **Type C: Passive Provisions** are passive structures and components with functions performed regardless the occurrence of PIEs and triggered sequences, implementing SSFs related to mechanical support, fluid boundary, building rooms/compartments, radioactive material barriers or containment, shielding, etc.

The term Passive Provision refers essentially to the same concept of IAEA’s SSG-30 “Design Provision”. The latter is a term that, in INVAP experience, is associated with a different wider meaning in the industry, applied to active SSCs as engineering provisions.

d) **Type D: Safety Monitoring Systems** implement the Human Machine Interface (HMI) regarding the information that participates in any of the following monitoring functions:

i. Provide information to characterize/identify the sequence following an AOO/IE and to allow an estimation of its effects, so that the operator can decide protective actions.

ii. Provide means to record, store and manage the information from Safety Monitoring.

Monitoring is related to SSCs of all type, to radiation protection and to the safety of workers not necessarily associated with specific SSCs.

e) **Type E: Support Systems** relevant to safety that provide supplies or material services to an SSC performing a safety function, allowing it to work. The failure of the support systems affects the functionality of the supported SSC by accountable means (effect and time-frame).

f) **Type F: Auxiliary Systems** relevant to safety that perform a function that impacts on conditions necessary for the safe operation of the reactor (Limiting Conditions for safe Operation, LCO), related to radiation protection, or to environment around SSCs. The latter could be for allowing operators interventions on SSCs, or with impact on SSCs’ availability, such as the control of water purity, ventilation of I&C rooms or lightning protection.

In line with the safety classification procedure Table III presents the preliminary list of the Specific Safety Functions of a reactor SSCs grouped according to the type of SSC.

Table III: Specific Safety Functions defined for the Reactor

Type of SSC	Name	Specific Safety Function description
Retention systems	Ret A	Retention by active ventilation of Air with dispersed radioactive material
	Ret W	Retention by active purification of Water with radioactive material
	Ret D	Control of Discharge or release of radioactive waste or radioactive effluents
	Ret P	Prevent the occurrence of conditions leading to the failure of a Barrier
Passive Provisions	Mechanical/process/civil	
	PP M A	Keep by Mechanical means the geometry of an Assembly, maintaining safety relevant cooling paths and/or distancing
	PP M B	Implement by Mechanical means an engineered fluid Boundary
	PP C	Implement a Civil structure housing or supporting safety relevant SSCs
	Radiological	
	PP P	Confine fuel meat by leak-tightness (component acting as Primary barrier)
	PP B	Confine by leak-tightness (component acting as physical Barrier)
	PP S	Shielding by a mechanical component or structure, or element of a building
	PP R	Provide passive Retention by physic-chemical means (e.g. pools water)
	PP D	Provide passive retention by Delay of material in convection
Safety Monitoring systems	SM G	Acquire, process and present in HMIs General information on safety relevant SSCs for operators to diagnose the plant status and decide actions
	SM RP	Acquire, process and present in HMIs Radio-Protection information
Support Systems	SS E	Provide Electrical supply and grounding
	SS O	Provide a supply Other than electrical power (e.g. compressed air, fuel, noble gasses, cooling water, hydraulic pressure)
Auxiliary Systems	AS H	Provide means to the Habitability of rooms (e.g. HVAC, lighting)
	AS RP	Provide Radio-Protection means as: zonification access controls, dosimeters management, decontamination devices, radioactive liquids drains
	AS E	Provide Emergency management means (e.g. lights and signaling for evacuation-sheltering)
	AS G	Provide General infrastructure of the facility (communication services, storage facilities and devices, handling tools, lightning protection, etc.)

2.4. Categorisation of functions

The functions required to fulfil the FSFs should be categorized on the basis of their safety significance, taking into account the three factors as presented in IAEA's standard SSG-30;

Factor 1: The severity of the consequences of the failure to perform the function;

Factor 2: The probability of occurrence of the IE for which the function is called upon;

Factor 3: The urgency of the contribution of the function.

Factor 1: the severity of consequences of the failure to perform, presented in terms of DiD levels is identifying the level in which it performs and assuming its failure leads to next DiD level, so:

- *High severity* is losing reactor protection, by failing to perform a FSF in accidental conditions (i.e. a PIE in DiD 3a, 3b or 4), leading to core damage or to radioactive releases.
- *Medium severity* is losing prevention, by failing to perform a FSF after an AOO (DiD 2), leading to a protection system triggering.

- *Low severity* is losing nominal operating conditions by failing to perform a FSF in NO (DiD 1) leading to the actuation of a limitation system.

If the failure of a function does not lead to the change in DiD level, it could also be considered within low severity of consequences.

The rule of categorization factor 1 is that safety category 1 is assigned to the functions with higher consequences of their failure. This can be summarized in Table IV.

Table IV: Severity of consequences of Safety Function failure assessed by DiD

Severity of the Consequence of SF failure	DiD Level reached during sequence after SF failure
HIGH	Exceeds DiD 3a, 3b or 4
MEDIUM	Exceeds DiD 2
LOW	Exceeds DiD 1 or does not change DiD level

Factor 2 is also presented in terms of DiD levels, by grouping IEs in DiD levels. If the IE is in a DiD level higher than DiD 3a (i.e. if the IE has a probability of occurrence lower than that of a DBA) the safety category is lower than the Safety Category expected by factor 1.

Factor 3 considers whether the function is intended for the long term, i.e. to reach a safe state, as opposed to the short term functions needed to reach a controlled state. For a safe state, functions are performed manually once the operator has diagnosed the scenario and assessed the convenience and viability of the use of specific SSCs, and the category is lower than the Safety Category expected for the functions pointing to short-term conditions (controlled state). The "urgency" is given by a time shorter than a "grace period" during which the operator is not expected to take decisions.

From previous paragraphs, the category of the Safety Function may be given by the DiD level exceeded after the Safety Function failure, and by the factor 3. Table V summarizes this.

Table V: Safety Function Category assessed by the three categorisation factors

DiD Level change after the Safety Function failure (factors 1 and 2 combined)	Safety Category	
	Short Term	Long Term (factor 3)
Exceeds DiD 3a	1	2
Exceeds DiD 2 or DiD 3b or DiD 4	2	3
Exceeds DiD 1 or does not change DiD level	3	Not categorised

2.5. Preliminary safety classification

The preliminary safety classification of SSCs is summarised in the following sub-sections, while a simplified scheme of the classification process is presented in Figure 2.

2.5.1. Preliminary Classification of SSCs type A

Reactor Systems are preliminarily classified by the highest Safety Category of the Safety Functions performed, i.e., the SSCs performing SFs of Safety Category N are preliminarily assigned Safety Class N, with N from 1 to 3.

2.5.2. Preliminary classification of SSCs other than type A

The preliminary safety classification of all types of SSCs other than type A, is performed without categorising the safety function the SSC performs. These safety functions are addressed as Specific Safety Functions, and defined (described) in Table III.

The key of the safety classification of SSCs is the consequences of their credible failure, assessing the severity of the consequences against several parameters, summarised in Table VI. Then high severity of consequences lead top SC 1, medium to SC 2, and low to SC 3.

The use of alternative assessment parameters allows for choosing the most efficient approach, keeping in mind that the rationale should be accountable.

Table VI: Severity of consequences based upon several criteria

Severity of the Consequence of FAILURE	**Alternative parameters**			
	DiD level	**Radiological criteria**	**Robustness criteria/ consequential failure**	**OLC**
HIGH	Exceeds DiD 3a	Exceeds a design criteria for acceptable doses in accident conditions for public or workers	Produces failure of a SC 1 SSC performing a SF in DiD 3a	Exceeds a Safety Limit
MEDIUM	Exceeds DiD 2	Exceeds a design criteria for acceptable doses in operational conditions for the public	Produces failure of a SC 2 SSC performing a SF in DiD 2 or 3b	Exceeds a Safety System Setting
LOW	Exceeds DiD 1	Exceeds a design criteria for acceptable doses in operation for workers or has a relevant radiological impact on the public	Produces the failure of other Items Important to Safety	Exceeds a Limiting Condition for safe Operation

The severity of the consequence of failures can be determined based upon which parameter is taken as indicator when exceeded: DiD Levels, Radiological criteria or Robustness criteria. OLCs may be seen as an alternative parameter to determine the severity of the consequence of failures, but actually is more a verification of consistency than a determination.

2.5.2.1. Retention Systems (type B)

The preliminary safety classification of these SSCs is based on the consequences of their credible failure, mainly with the column of radiological criteria.

2.5.2.2. Passive Provisions (type C)

This type of SSCs "*are preliminarily classified directly because the significance of their credible failure fully defines its safety class without any need for detailed analysis of the category of the associated safety function*" (SSG-30 quote). This significance is assessed by the severity of the consequences of their failure, using several alternative parameters. For Passive Provisions related to the SSCs of a reactor, the DiD level is the preferable parameter.

2.5.2.3. Safety Monitoring Systems (type D)

The preliminary safety classification is performed in line with IEC 61226 standard.

A Safety Monitoring System is assigned Safety Class 2 when the provided information requires immediate action of the operator to avoid MEDIUM severity consequence. In all other cases the Safety Monitoring System will be assigned Safety Class 3.

In INVAP reactor designs there are no cases requiring immediate operator actuation to avoid HIGH severity of consequences and there are no SC 1 Safety Monitoring Systems.

2.5.2.4. Support systems (type E)

The preliminary classification is by assigning the Safety Class of the supported SSC.

2.5.2.5. Auxiliary systems (type F)

Auxiliary systems are not associated with a single/specific SSCs/process. Safety Class is assigned by the severity of the consequences of their failure, using several alternative parameters. Within best practice, no credible failure of an Auxiliary System would lead to HIGH severity of consequences.

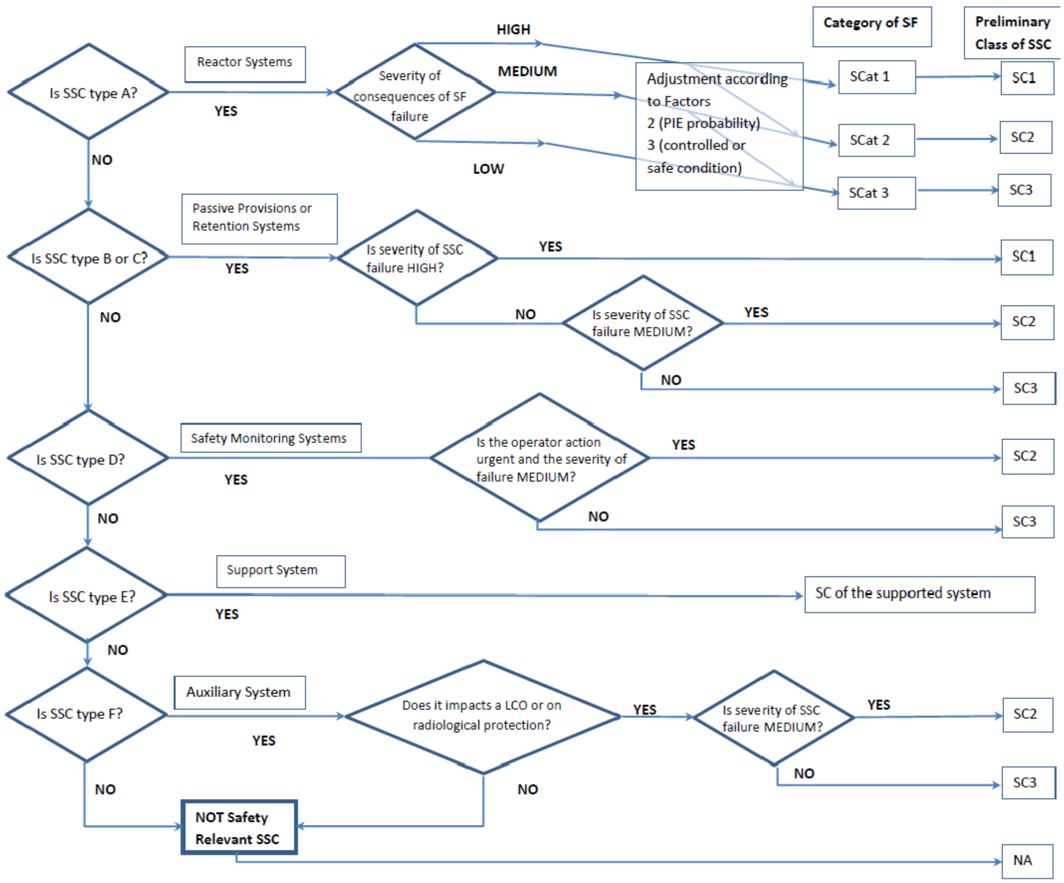

Figure 2: Diagram of the Preliminary Safety Classification Process

2.6. Rules for safety class reduction

The preliminary safety classification as described would already be acceptable in terms of Safety. However, according to best international practice, there is room for optimising the design by amending the initial safety classification. In IAEA in SSG-30, there are guidelines to "*permit the SSC to be moved into a lower class, provided that its expected reliability* [in performing the safety function] *can be demonstrated*". See SSG-30, section 3, para 3.20.

The "amendment" is to be made by accountable rules of class reduction. The proposed class reduction rules and rationale on keeping the reliability are:

a) SSCs already in operation (not affected by the IE), given that the probability of spontaneous failure is always lower than Failure-rate on demand.

b) SSCs that perform a function as a diverse implementation of another SSC, given that the latter keeps the preliminary class. The addition of a second SSC performing the same safety function can only increase the reliability of the function.

c) SSCs featuring failure modes with delayed effects on the safety function. Delay allows operator intervention to deal with the failure (e.g. reverse the failure by repair).

d) SSCs featuring failure modes with negligible effects on the safety function, that is, the function is still effectively performed in the event of this failure.

These Class Reduction Rules may be applied to components, equipment, subsystems (section / part of systems) and to complete systems.

The Safety Class amendment leads to the final Safety Class, as the final indicator of the safety relevance and connection with requirements to be applied to a specific SSC.

2.7. Other aspects of SSCs safety classification

Within a safety approach, a “system” comprises the elements that effectively contribute to perform a safety function. Its components are identified to reach “integrality” (the terms “comprehensiveness”, “wholeness” and “functional completeness” were also considered).

On the other hand, elements are tagged within a System Breakdown Structure (SBS) as a system, a subsystem/circuit (part of another system) or a support system, based on the needs of engineering and management. Consequently, the denomination “system” of the SBS does not necessarily agree with the “systems” named in safety assessments.

All the elements of the systems “according to safety concept”, “performing safety functions” are part of the SBS, and the denomination is not an issue as long as the concepts of “integrality” and “granularity” are accounted for in the methodologies of Safety Classification and derivation of safety requirements.

Regarding “integrality”, the components participating in performing a given safety function may belong to different “systems” as presented in the SBS, but should be described in an integral way in order to retain the functional description (e.g. in Safety Design Basis docs).

As an example of this integrality in a reactor project, the shutdown function integrates:

- the sensors and measuring chains catering the FRPS (embedded in several systems),
- the FRPS itself (4110-First Reactor Protection System), through the Actuation Logic,
- the actuators of the FSS (0200-First Shutdown System and Reactivity Control) and
- the elements that implement or condition the shutdown function, including the Control Rod Drive, the stem, the seal box, and pass-through (Control rods penetration device of the 0410-Reflector vessel) the absorber plate and the guide box (0100-Reactor Core).

On the other hand, the adequate “granularity” of the SBS refers to the level of detail on the elements (components, equipment, subsystems, sections or parts of systems) allowing to distinguish the functional role and the type of SSC, and to assess the consequences of failures, allowing a safety classification.

The SBS must be compatible with the need of granularity and integrality of systems.

3. Conclusions

This paper presented an accountable structured method for performing safety classification of SSC important to safety consistent with the concepts of safety classification set out in IAEA standards [1] and [2], while developing relevant improvements:

- Systematic use of the Defence in Depth (DiD) safety concept for categorising functions.
- Extending the scope covering all SSCs of a reactor plant design, not only the ones performing the Fundamental Safety Functions on the nuclear reactor.
- Development of an approach allowing the verification of completeness and consistency of the list of Safety Functions, and a systematic view of Specific Safety Functions.
- Provides accountability to the practice of “safety class reduction” to assorted SSC, by identifying rules with explicit rationale.

Acknowledgements

The authors wish to thank all the seasoned experts that took part on the development and thorough review of the methodology, particularly the Nuclear Technology Board of INVAP.

References

[1] IAEA, Safety Classification of Structures, Systems and Components in Nuclear Power Plants - Specific Safety Guide. SSG-30. VIENNA, 2014.
[2] IAEA, Safety of Research Reactors - Specific Safety Requirements. SSR-3. Vienna, 2016.