A REVIEWED APPROACH TO SAFETY CLASSIFICATION OF SSC IN NUCLEAR REACTORS

N. A. MASRIERA, A.S. DOVAL, J.A. WEIGANDT

INVAP, Nuclear Business Division

TRTR – IGORR Conference, 2023

DEFINITIONS

Safety Class: Classes into which SSCs are assigned on the basis of their functions and their safety significance (IAEA glossary)

Safety Categories: assignation on the functions based on their safety significance.

Why classes and categories?

Nuclear Safety demonstration is functional. Safety relevance is functional➔ S Cat of SF.

There may be more than one system performing the same SF (e.g. FSS, SSS)

A system of “diverse line” is assigned a different Safety Class

Actually there are several engineering solutions allowing a lower class

Terms introduced:

SSC, Type of: Structure, System and Component of the design, identification of an SSC according to the role it plays in the safety demonstration process.

Preliminary classification: Safety Class assigned by the classification methodology before the application of class reduction rules.

Class reduction: Process by which an SSC, assigned to a preliminary safety class, can be reassigned to a lower class (keeping reliability on its function).

Passive Provisions: Passive elements that perform the same function in operational (including FP steady state - Power ROS) and accidental scenarios.

It’s the same **concept** described in IAEA SSG-30 as “design provisions”.

INTRODUCTION

Safety Classification is a top down process:

- understanding of plant functional design,
- safety assessments (safety analyses and radiological assessments),
- assigning a Safety Class to all the safety relevant SSCs of the design (all type of SSCs, be them related to the reactor or to radiological safety).

Based on deterministic safety assessments complemented by insights from probabilistic assessment and engineering judgment.

DiD is the key for the safety classification of reactor systems.

The outcome of safety classification process (the Safety Class of each SSC) is an input to define safety requirements.

Definition of types of SSC

Six types of SSCs performing safety functions are identified :

Type A: **Reactor Systems** actively perform a **Safety Functions derived from the Fundamental Safety Functions**, implemented within DiD levels.

Type B: Retention Systems actively perform retention of radioactive material, by ventilation and purification systems.

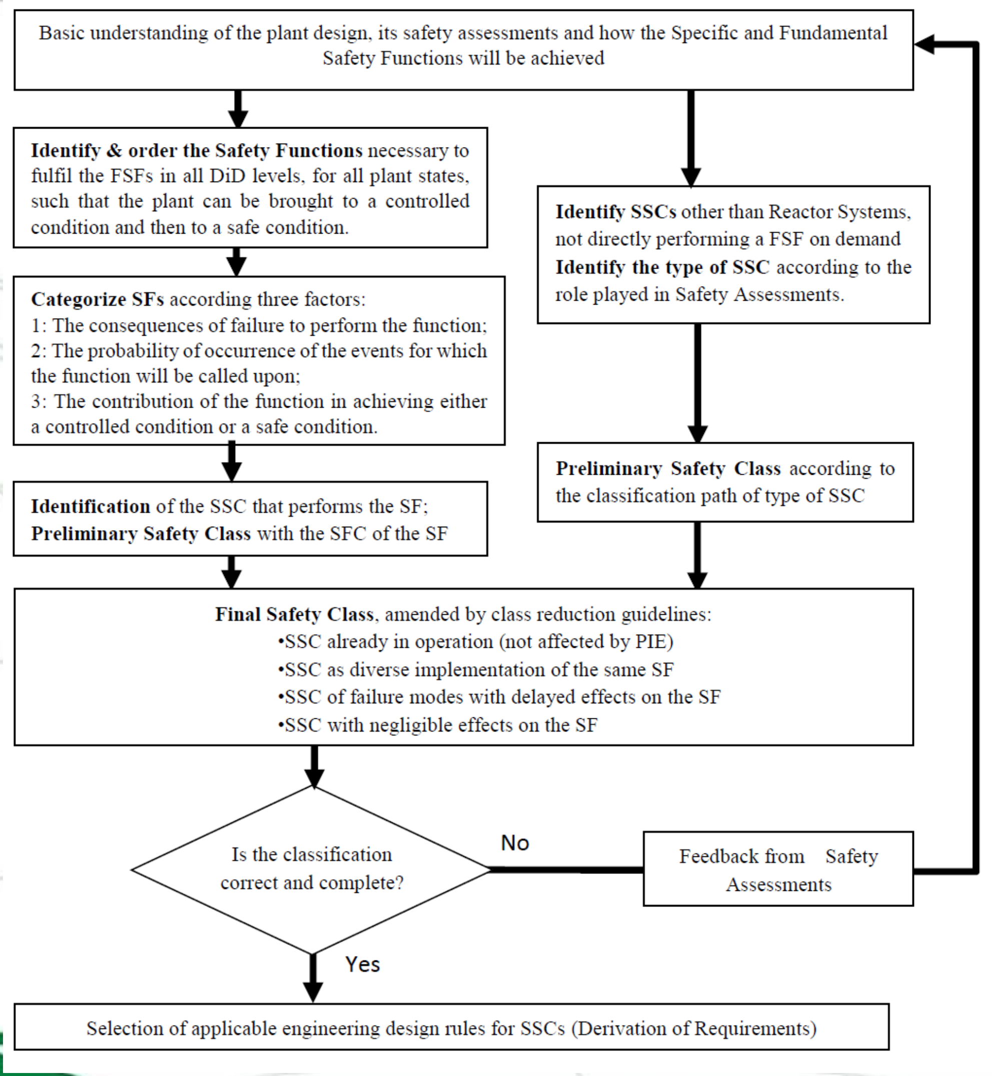
Type C: Passive Provisions, passive elements (generally structures / components) as mechanical support, fluid boundary, shielding, etc.

Type D: Safety Monitoring systems implement the Human Machine Interface regarding the provision and handling of information.

Type E: Support Systems provide a supply or material services to a SSC performing a safety function, allowing it to work.

Type F: Auxiliary systems impact on a Limiting Condition for safe Operation, or on radiation protection within the plant. Not on a single/specific SSCs/process.

Simplified flow-chart of the categorisation - classification procedure



Basic understanding of the plant design, its safety assessments and how the Specific and Fundamental Safety Functions will be achieved

Identify & order the Safety Functions necessary to fulfil the FSFs in all DiD levels, for all plant states, such that the plant can be brought to a controlled condition and then to a safe condition.

Categorize SFs according three factors:
1: The consequences of failure to perform the function;
2: The probability of occurrence of the events for which the function will be called upon;
3: The contribution of the function in achieving either a controlled condition or a safe condition.

Identification of the SSC that performs the SF;
Preliminary Safety Class with the SFC of the SF

Identify SSCs other than Reactor Systems, not directly performing a FSF on demand
Identify the type of SSC according to the role played in Safety Assessments.

Preliminary Safety Class according to the classification path of type of SSC

Final Safety Class, amended by class reduction guidelines:
- •SSC already in operation (not affected by PIE)
- •SSC as diverse implementation of the same SF
- •SSC of failure modes with delayed effects on the SF
- •SSC with negligible effects on the SF

Is the classification correct and complete?

No

Feedback from Safety Assessments

Yes

Selection of applicable engineering design rules for SSCs (Derivation of Requirements)

Identification and ordering of safety functions

The safety assessments (safety analysis and radiological assessments) are deterministic functional analyses on the SSCs performing safety functions.

- **Safety Functions**, required to actively perform the Fundamental Safety Functions by the design. Credited in the deterministic safety analysis, include functions performed at all corresponding DiD levels.

Categorised before assigning Safety Classes to SSCs

- **Specific Safety Functions**, considered in safety assessments outside the DiD scheme of levels, including: radiological protection functions on inventories other than the core; functions of passive provisions; monitoring functions to allow operator safe decisions, support and auxiliary functions.

Useful for a consistent description of safety aspects of SSCs **and for performance assessment**

Fundamental Safety Functions - Safety Functions

- Reactivity control (shutting down)
- Heat removal from the reactor (decay heat)
- Confinement of radioactive material (of the reactor core).

FSFs are “entities” at a conceptual level

When taken to the level of systems and components that perform them, the **Fundamental Safety Functions are unfolded into Safety Functions**

SF Name	Safety Function Description	DiD Level	Safety Category	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 PCDA**	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**.	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 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**.	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 reactor **core** or fissile **targets** damage	4	2	b

Table 2: Safety Functions ordering table

DiD level (Plant State)	**Control by I&C C**	**Reactivity R**	**Heat removal and transfer K**				**Confinement B**	
			Water inventory W	H removal & transfer to short-term UHS		H transfer to **L**ong-term UHS	Barriers	Retention
				Core	Fissile **T**arget			
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) **1**	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)	C6	(*3)	(*3)	(*3)	(*3)	(*3)	(*2)	B

(*1): by Passive Provisions Primary Barrier – cladding (no further retention needed)

(*2): in extended LOEP by Reactor Containment

(*3): scenarios in which R and K safety functions are performed manually, with the operator using the SSCs chosen as convenient and viable. No “new” safety function or SSC .

Categorisation of functions

The functions required for fulfilling the FSFs are categorized on the basis of three factors as presented in IAEA’s standard SSG-30;

Factor 1 **(main factor)**: The severity of the consequences of the failure to perform the function;

Factor 2: The probability of occurrence of the initiating event for which the function will be called upon;

Factor 3: The significance of the contribution of the function in achieving either a controlled (short term) condition or a safe condition.

Factor 1:
consequences of failure to perform the function

Presented in terms of DiD levels on the basis of the worst consequences that could arise if the function were not performed.

Consequence Severity of the 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

Factors 2 and 3

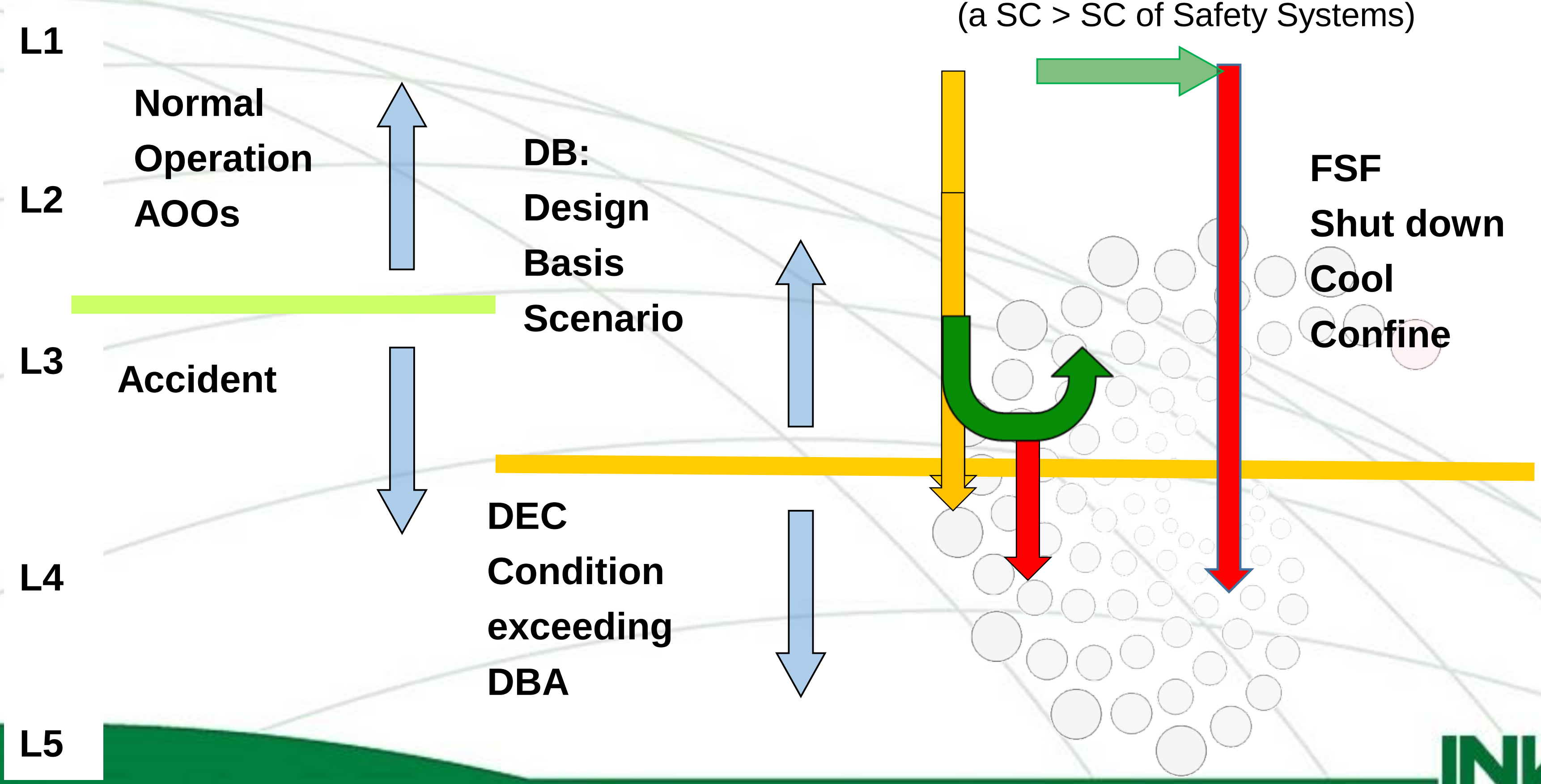
Factors 2: if the IE is in a DiD level higher than DiD 3a (probability lower than a DBA) the Safety Category is lower than the one expected by factor 1. It is also presented in terms of DiD levels.

Factor 3: if the Safety Function is demanded to achieve a safe condition, allowing manual action without urgency, Safety Category is lower than the one expected for the functions pointing to controlled conditions.

DiD Level change after the SF failure (factors 1 and 2 combined)	**Safety Category**	
	Short term - Controlled State	**Long term - Safe State (factor 3)**
Exceeds DiD 3a	1	2
Exceeds DiD 2**, DiD 3b or DiD 4**	2	3
Exceeds DiD 1 or does not change DiD level	3	Not categorised

Preliminary Safety Class: SC 1

In PWR NPPs, the coolant Pressure Boundary may be assigned a “super-class” (a SC > SC of Safety Systems)



L1

L2

L3

L4

L5

Normal

Operation

AOOs

Accident

DB:

Design

Basis

Scenario

DEC

Condition

exceeding

DBA

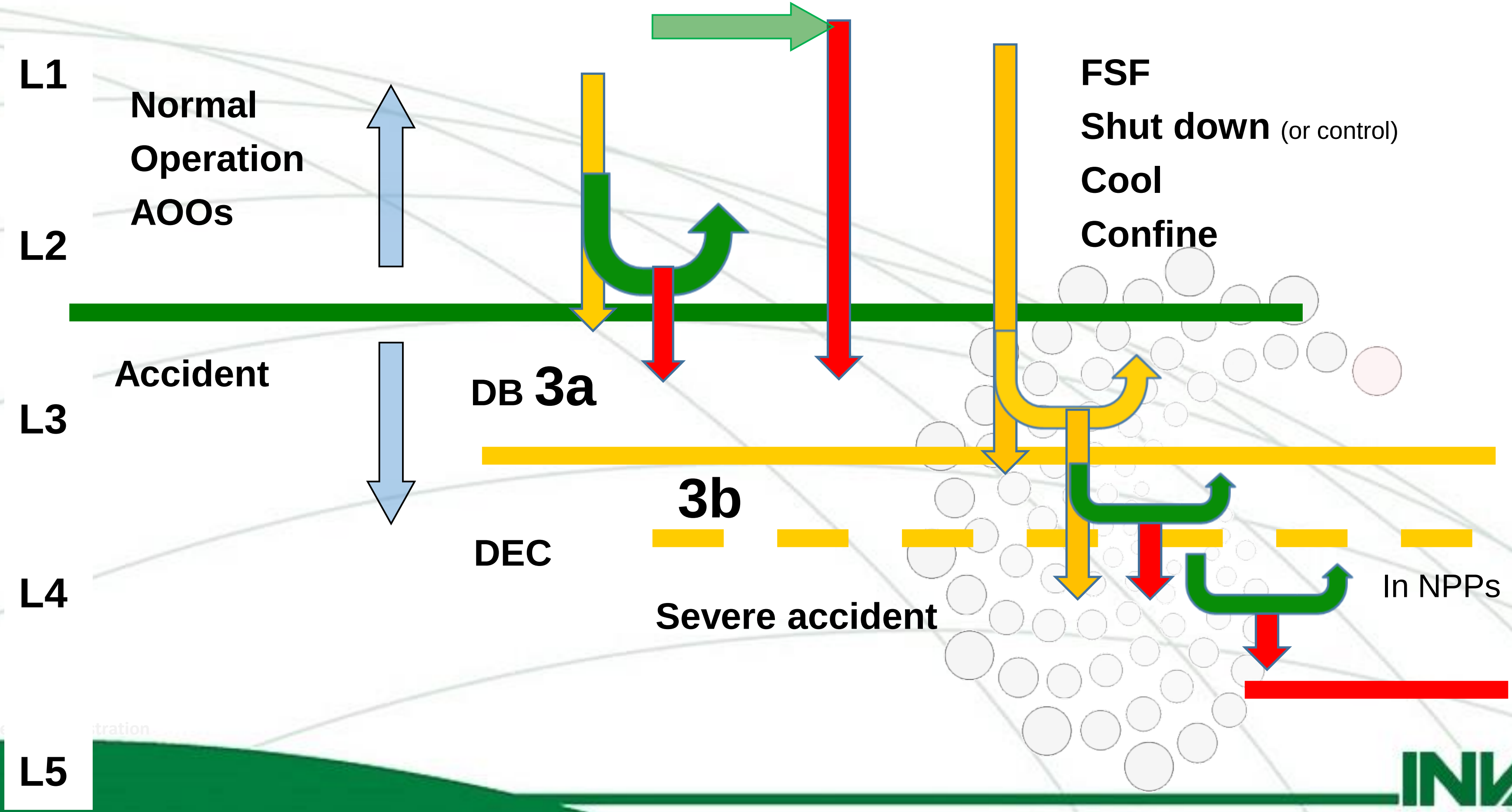
FSF

Shut down

Cool

Confine

Preliminary Safety Class: SC 2



L1

Normal

Operation

AOOs

L2

Accident

L3

L4

L5

DB 3a

3b

DEC

Severe accident

FSF

Shut down (or control)

Cool

Confine

In NPPs

Preliminary Classification of other type of SSCs

Preliminary Safety **Class** of Reactor Systems = Safety **Category** of the Safety Function it performs.

Other type of SSCs are classified directly, without categorizing the safety function

The key of the safety classification approach is the consequences of the credible failure of the SSC, assessed against several parameters.

This allows choosing the most efficient (practical) approach, keeping in mind that the rationale should be accountable.

If the SSC performs several functions, it is assigned the highest.

Consequences of failure, assessed against several parameters

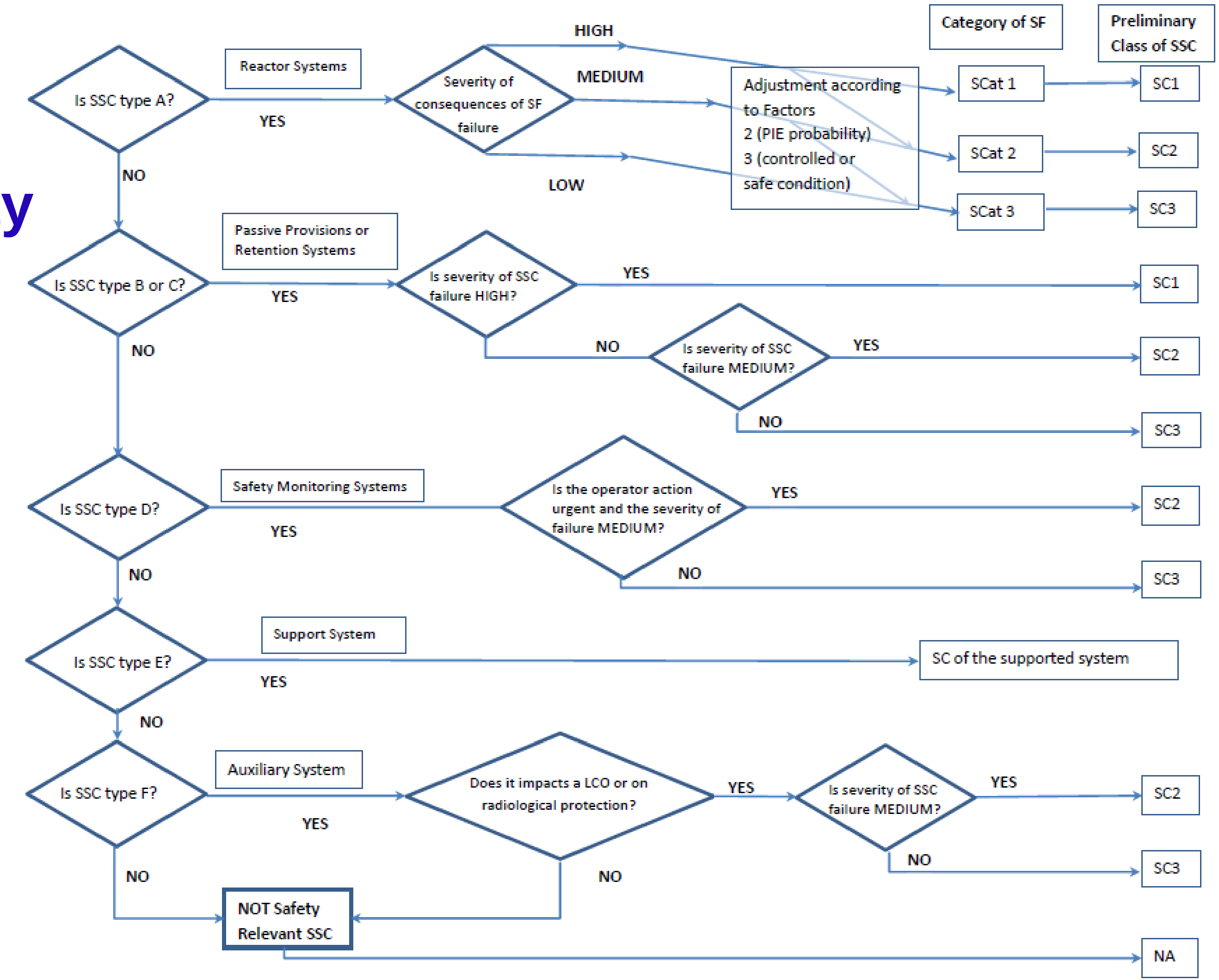
Consequence Severity of FAILURE	Alternative parameters			
	DiD Level	Radiological criteria	OLCs	Robustness Criteria / consequential failure
HIGH	Exceeds DiD 3	Exceeds acceptable doses of accident conditions for public or workers	Exceeds a Safety Limit	Produces failure of a SC 1 SSC performing a FSF in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

Consequences of failure, assessed against several parameters

Radiological Severity of Consequence FAILURE	E, Effective dose to the public	E, Effective dose to workers
HIGH	E > 10 mSv	E > 50 mSv
MEDIUM	0.1 mSv < E ≤ 10 mSv	6 mSv < E ≤ 50 mSv
LOW	0.04 mSv < E ≤ 0.1 mSv	2mSv < E ≤ 6 mSv

Severity of consequences of the failure of the SSC	Safety Class
HIGH	**SC 1**
MEDIUM	**SC 2**
LOW	**SC 3**

Diagram of the Preliminary Safety Classification Process of other type of SSCs



Category of SF

Preliminary Class of SSC

Is SSC type A?

Reactor Systems

YES

Severity of consequences of SF failure

HIGH

MEDIUM

LOW

Adjustment according to Factors 2 (PIE probability) 3 (controlled or safe condition)

SCat 1

SCat 2

SCat 3

SC1

SC2

SC3

NO

Is SSC type B or C?

Passive Provisions or Retention Systems

YES

Is severity of SSC failure HIGH?

YES

SC1

NO

Is severity of SSC failure MEDIUM?

YES

SC2

NO

SC3

NO

Is SSC type D?

Safety Monitoring Systems

YES

Is the operator action urgent and the severity of failure MEDIUM?

YES

SC2

NO

SC3

NO

Is SSC type E?

Support System

YES

SC of the supported system

NO

Is SSC type F?

Auxiliary System

YES

Does it impacts a LCO or on radiological protection?

YES

Is severity of SSC failure MEDIUM?

YES

SC2

NO

SC3

NO

NO

NOT Safety Relevant SSC

NA

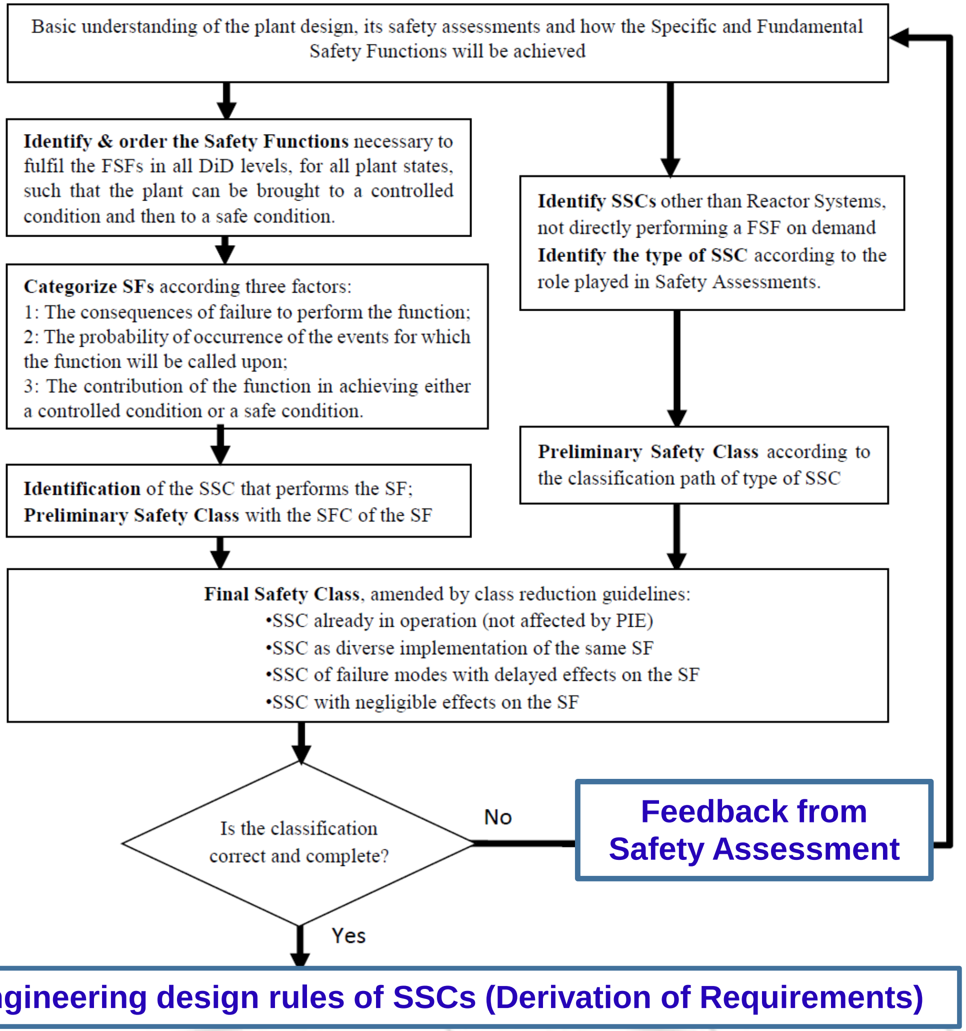
Rules for safety class reduction

There is room for optimising the design, amending classification to "*permit the SSC to be moved into a lower class, provided that its expected reliability* [in performing the safety function] *can be demonstrated*". SSG-30, s 3., para 3.20.

- SSCs already in operation (not affected by the IE) - the probability of spontaneous failure is always lower than failure-rate on demand.
- SSCs implementing the same function as another SSC (the latter keeps preliminary class) - adding an SSC with same Function can only increase the reliability.
- SSCs with failure modes of delayed effects on safety function, allowing the operator intervention to cope with the failure (e.g. by repair).
- SSCs with failure modes with negligible effects on the safety function, that is, the function is still performed in the event of this failure.

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

Final safety classification



Basic understanding of the plant design, its safety assessments and how the Specific and Fundamental Safety Functions will be achieved

Identify & order the Safety Functions necessary to fulfil the FSFs in all DiD levels, for all plant states, such that the plant can be brought to a controlled condition and then to a safe condition.

Categorize SFs according three factors:
1: The consequences of failure to perform the function;
2: The probability of occurrence of the events for which the function will be called upon;
3: The contribution of the function in achieving either a controlled condition or a safe condition.

Identification of the SSC that performs the SF;
Preliminary Safety Class with the SFC of the SF

Identify SSCs other than Reactor Systems, not directly performing a FSF on demand
Identify the type of SSC according to the role played in Safety Assessments.

Preliminary Safety Class according to the classification path of type of SSC

Final Safety Class, amended by class reduction guidelines:
- SSC already in operation (not affected by PIE)
- SSC as diverse implementation of the same SF
- SSC of failure modes with delayed effects on the SF
- SSC with negligible effects on the SF

Is the classification correct and complete?

No

Feedback from Safety Assessment

Yes

Selection of applicable engineering design rules of SSCs (Derivation of Requirements)

Other aspects around Safety Classification

Within a safety approach, “systems” are defined by the elements that contribute to perform a safety function: “comprehensiveness” (wholeness / integrality)

Elements tagged as a **system** within the System Breakdown Structure, a subsystem / circuit (part of) or support based on engineering needs and management decisions.

“System” of SBS may not agree with “systems” of safety docs. It is not an issue if the concepts of “granularity” and “comprehensiveness” are accounted for.

Granularity: identifying objects **in the SBS** at a level with sufficient detail allowing to distinguish the functional role and the type of SSC, to assess consequences of failures → safety class → requirements.

Comprehensiveness: objects integration **in the Safety Design Basis documents.** Components participating in the performance of the Safety Function may belong to different “systems” as presented in the SBS.

Other aspects around Safety Classification

Example

*In some RR the **comprehensiveness of the shutdown function includes:***

the sensors and measuring chains catering the FRPS (embedded in several systems),

the FRPS itself (4110-First Reactor Protection System), through the Actuation Logic, reaching the actuators of the FSS (0200-First Shutdown System and Reactivity Control)

elements that implement or condition the function: 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).

Conclusions

The Safety Classification Methodology presented is based on the approach proposed by IAEA (2012) and on the practice of INVAP as a Nuclear Designer – Vendor, and is applicable to any size of water-cooled, nuclear reactor with cladded-fuel.

It is essentially accountable in different aspects:

Treatment of functions, categorization factors, treatment of probability of demand, class reduction rules, type of SSCs to classify…

The comparison with other classification approaches can be further analysed / discussed, considering all specific aspects.

Thank you for your time

INVAP