Safety Classification of Systems, Structures, and Components

S. Michael Modro

Based on presentation of Bernard POULAT

Joint IAEA-ICTP Essential Knowledge Workshop on Nuclear Power Plant Design Safety-Updated IAEA safety Standards

9-20 October 2017

Trieste, Italy

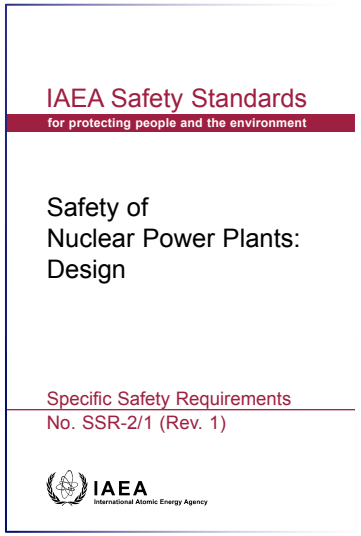
Outline

- Objective of the safety classification
- General approach
- Safety classification process
  - Safety functions performed by systems
  - Design provisions
  - Definition of safety classes
- Assignment of SSCs to safety classes
- Applicable engineering design rules

Requirement 10: Assessment of engineering aspects (2/7)

- Where innovative improvements beyond current practices have been incorporated into the design, it shall be determined whether
  - compliance with the safety requirements has been demonstrated by an appropriate programme of research,
  - analysis and testing complemented by a subsequent programme of monitoring during operation.
- It shall be determined whether a **suitable safety classification** scheme has been formulated and applied to structures, systems and components.
  - Does the safety classification scheme adequately reflects the importance to safety of structures, systems and components, the severity of the consequences of their failure, the requirement or them to be available in anticipated operational occurrences and accident conditions?
  - Are the systems and components adequately qualified?
  - Does the scheme identifies the appropriate industry codes and standards and the regulatory requirements to be applied in the design, manufacturing, construction and inspection of engineered features, in the development of procedures and in the management system for the facility or activity.

General Approach



Requirement 4: Fundamental Safety Functions

- Fulfilment of the following fundmental safety functions shall be ensured for all plant states:
  - control of reactivity
  - removal of heat from the reactor and from the fuel store and
  - confinement of radioactive material, shielding against radiation and control of planned radioactive releases, as well as limitation of accidental radioactive releases.

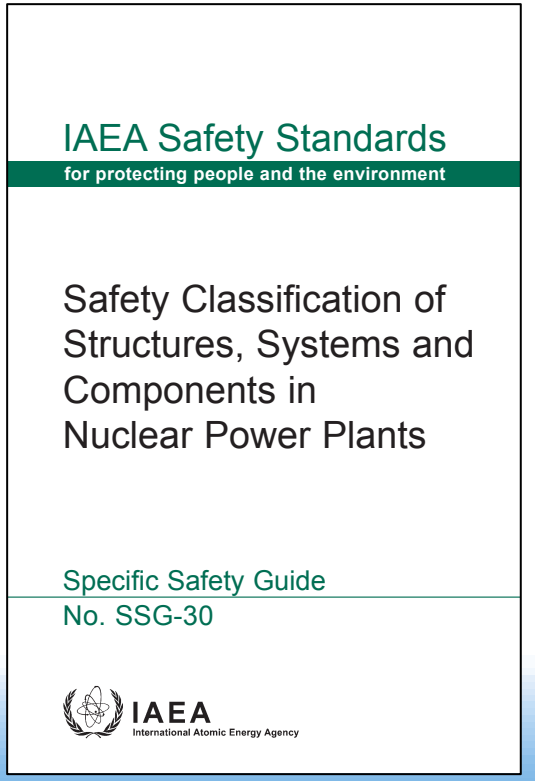
Requirement 22: Safety Classification

- All items important to safety shall be identified and shall be classified on the basis of their function and their safety significance.

Preliminary considerations

- **Safety classification** has been implemented for long time as a prescriptive set of rules **based on good engineering practices** that linked specific structures, systems and components to well identified rules for design, manufacturing and operating.

- The IAEA with SSG-30 provides a rationale for the creation of a classification scheme to comply with the requirements established in SSR-2/1 Rev 1.



Objective

- Safety classification aims to **identify and classify SSCs that are needed to protect people and the environment** from harmful effects of ionizing radiation, on the basis of their roles in preventing accidents, or limiting the radiological consequences of accidents.
- On the basis of their classification, SSCs are then designed, manufactured, operated, tested and inspected in accordance with established processes that ensure that expected levels of safety performance are achieved.

- The method for classifying the safety significance of items important to safety shall be based primarily on deterministic methods complemented, where appropriate, by probabilistic methods, with due account taken of factors such as:

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

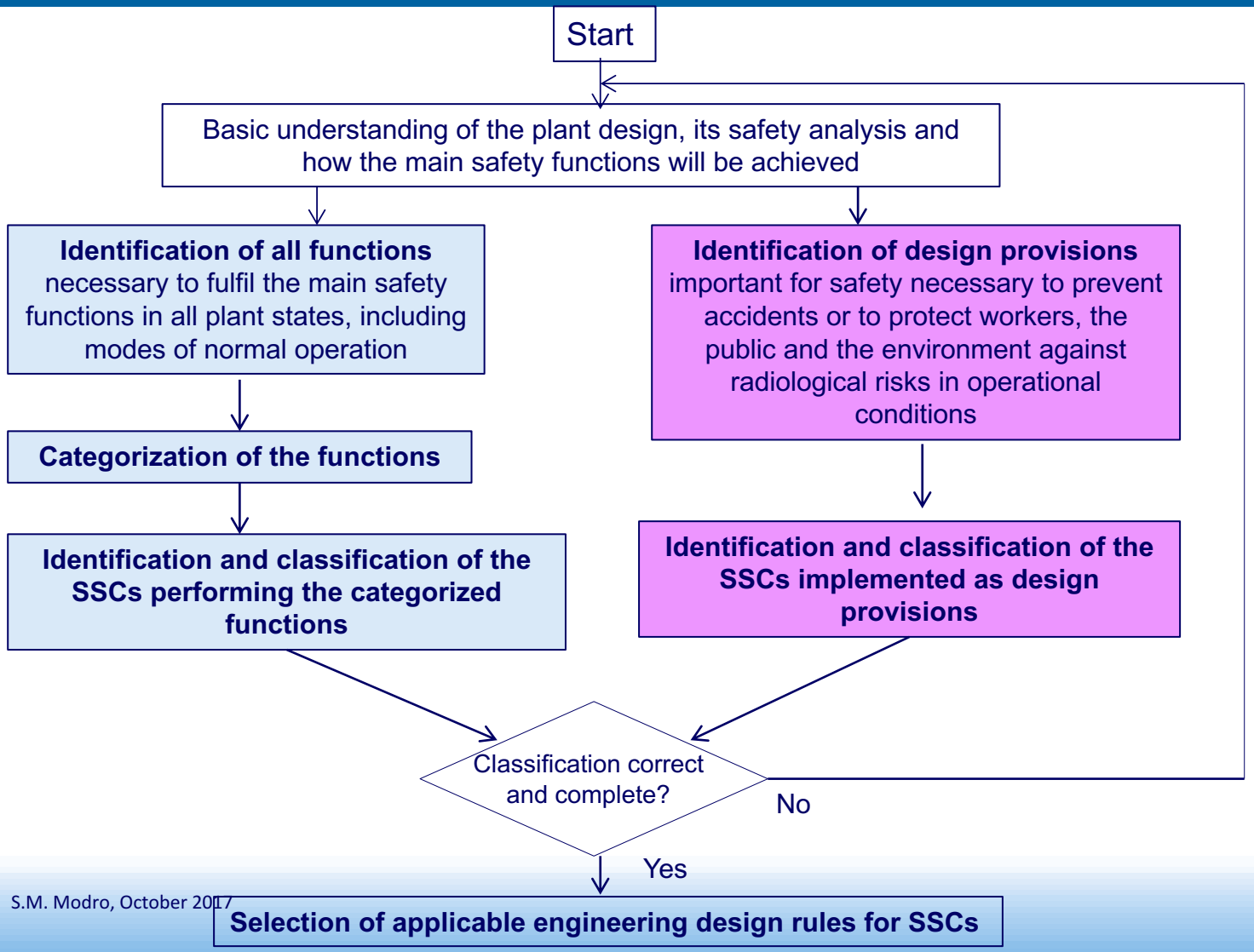
(b) The consequences of failure to perform a safety function;

(c) The frequency with which the item will be called upon to perform a safety function;

(d) The time following a postulated initiating event at which, or the period for which, the item will be called upon to perform a safety function.

- Prior starting the safety classification process, following inputs are necessary:
  - Radiological releases limits established by the Regulatory Body for operational conditions and for accident conditions
  - Plant systems description
  - Plant states definition and categorization
  - Postulated Initiating Events (PIEs) considered in the design with their estimated frequency of occurrence
  - Accident analysis
  - How the concept of defence in depth is implemented

Classification Process



SSCs necessary to accomplish the Fundamental Safety functions for different plant states.

Design features to "practically eliminate" some very severe conditions
Prevention of accidents
Protection of safety systems and safety features from hazards
Features to facilitate accident management

Function categorization

Function categorization makes easier the review of the safety classification by providing a classification/ranking which is not system dependent.

Function categorization makes the system classification clearer and more consistent by identifying all the systems that have to operate together to accomplish a particular function.

Function categorization has to be understood as a useful tool for the classification, but not strictly necessary.

Categorization can replace classification when the design is still insufficiently developed, as for example at the conceptual stage when all systems are not yet designed.

Categorization of a function, and later, classification of all the systems (necessary to accomplish a single function) in a same safety class does not preclude assigning the associated SSCs in different safety classes provided their individual safety significance not be the same.

Identification

Functions to be categorized are those required to achieve the main safety functions for the different plant states (operational conditions and accident conditions). For accident conditions, functions are those that are credited in the safety analysis.

Although the main safety functions to be fulfilled are the same for every plant state, the functions to be categorized should be identified with respect to each plant state separately.

It is recommended to detail functions as much has needed to cover all the different actions to be accomplished by the systems in the different plant states. So the number of functions is usually limited at a conceptual stage but is growing when the design is developing.

.

Identification

Fundamental Safety Function	Functions to be categorized for the different plant states
Control of Reactivity	R1 - Maintain core criticality control
	R2 - Shutdown and maintain core sub-criticality
	R3 - Prevention of uncontrolled positive reactivity insertion into the core
	R4 - Maintain sufficient sub-criticality of fuel stored outside the RCS but within the site
Heat removal	H1 - Maintain sufficient RCS water inventory for core cooling
	H2 - Remove heat from the core to the reactor coolant
	H3 - Transfer heat from the reactor coolant to the ultimate heat sink
	H4 - Maintain heat removal from fuel stored outside the reactor coolant system but within the site
Confinement of radioactive material	C1 - Maintain integrity of the fuel cladding
	C2 - Maintain integrity of the Reactor Coolant Pressure Boundary
	C3 – Limitation of release of radioactive materials from the reactor containment
	C4 – Limitation of release of radioactive waste and airborne radioactive material
EXtra	X1 –Protection and prevention against effects of hazard
	X2 - Protect of workers against radiation risks
	X3 - Limit the consequence of hazard
	X4 – Plant operation in accident conditions and monitoring of plant parameters
	X5 - Monitor radiological releases in normal operation
	X6 - Limits and conditions for normal operation

Can be used as a generic list of functions for pressurized water reactor.
Can be used for early classification but has to be more developed once the design is more detailed.
For classification purpose, those functions need to be defined for the different plant states taking into account that one single function is often accomplished by different systems, as generally requested by the Defense in depth concept.

Identification

Control of Reactivity	R1 – Maintain core criticality control	R-1.1: Control of RCS boric acid concentration
		R-1.2: Control rod position
		R-1.3: Control reactor power distribution
		R-1.4: Control reactor thermal power
		R-1.5: Control linear power density
		R-1.6: Control Pellet Clad Interaction risk
		R-1.7: Control Departure from Nucleate Boiling risk
		R-1.8: Limit reactor thermal power
		R-1.9: Limit linear power density
		R-1.10: Limit Pellet Clad Interaction risk
		R-1.11: Limit Departure from Nucleate Boiling risk
		R-1.12: Reduce reactor power
	R2 - Shutdown and maintain core sub-criticality	R-2-1: Fast negative reactivity insertion into reactor core (reactor trip)
		R-2 2: Injection of high borated water into RCS at high pressure (e.g., in case of anticipated transients without SCRAM)
		R-2 3: Injection of high borated water into RCS at medium and low pressure in case of DBA
		R-2.4: Compensate for reactivity increase during plant cooldown to the safe shutdown state by increasing the boric acid concentration in the RCS
	R3 - Prevention of uncontrolled positive reactivity insertion into the core	R-3.1: Restrict feedwater flow to SGs after reactor trip
		R-3.2: Isolation of feedwater supply to a damaged SG
		R-3.3: Prevent SG draining to RCS in case of SG tube rupture
		R-3.4: Prevent uncontrolled SG depressurization - Stop steam flow to turbine
		R-3.5: Prevent uncontrolled SG depressurization - Stop steam flow to atmosphere
		R-3.6: Prevent uncontrolled SG depressurization - Stop steam flow to main steam system
		R-3.7: Stop RCS forced flow to limit heat exchange in the SG
		R-3.8: Prevent component cooling water flow to RCS through leakage on heat exchanger (at low RCS pressure)
		R-3.9: Stop demineralized water make-up to RCS
	R4 - Maintain sufficient sub-criticality of fuel stored outside the RCS but within the site	R-4.1: Control of spent fuel pool water boric acid concentration

Categorization of functions

- **Practically, for each PIE, functions necessary to control or mitigate the consequences are identified and categorized.**
- **The categorization of functions is performed to reflect the safety significance of every function.**

Safety significance is assessed by screening the following factors:

- (1) The consequences of failure to perform the function;
- (2) The frequency of occurrence of the postulated initiating event for which the function will be called upon;
- (3) The significance of the contribution of the function in achieving either a controlled state or a safe state.

3 levels of severity: high, medium and low

Categorization of functions

Lead directly to a release of radioactive material that exceeds the limits for design basis accidents accepted by the regulatory body.

Lead to a release of radioactive material below the limits for design basis accidents accepted by the regulatory body but higher than those established for anticipated operational occurrences.

Lead to an off-site release of radioactive material not exceeding the releases authorized for normal plant operation, but could lead to doses to workers above the authorized limits.

Functions credited in the safety assessment of	Severity of the consequences of the failure of the function		
	High	Medium	Low
AOO	C1	C2	C3
DBA short term	C1	C2	C3
DBA	C2	C3	C3
DEC	C2 or C3	NC	NC

Categorization of functions

Safety category 1:

- **Any function that is required to reach the controlled state after an anticipated operational occurrence or a design basis accident and whose failure, when challenged, would result in consequences of 'high' severity.**

Safety category 2:

- **Any function that is required to reach a controlled state after an anticipated operational occurrence or a design basis accident and whose failure, when challenged, would result in consequences of 'medium' severity; or**
- **Any function that is required to reach and maintain for a long time a safe state and whose failure, when challenged, would result in consequences of 'high' severity; or**
- **Any function that is designed to provide a backup of a function categorized in safety category 1 and that is required to control design extension conditions without core melt.**

Categorization of functions

Safety category 3:

- **Any function that is actuated in the event of an anticipated operational occurrence or design basis accident and whose failure, when challenged, would result in consequences of 'low' severity; or**
- **Any function that is required to reach and maintain for a long time a safe state and whose failure, when challenged, would result in consequences of 'medium' severity; or**
- **Any function that is required to mitigate the consequences of design extension conditions, unless already required to be categorized in safety category 2, and whose failure, when challenged, would result in consequences of 'high' severity; or**
- **Any function that is designed to reduce the actuation frequency of the reactor trip or engineered safety features in the event of a deviation from normal operation, including those designed to maintain the main plant parameters within initial conditions of the accident analysis.**

Categorization of functions

Safety category 3:

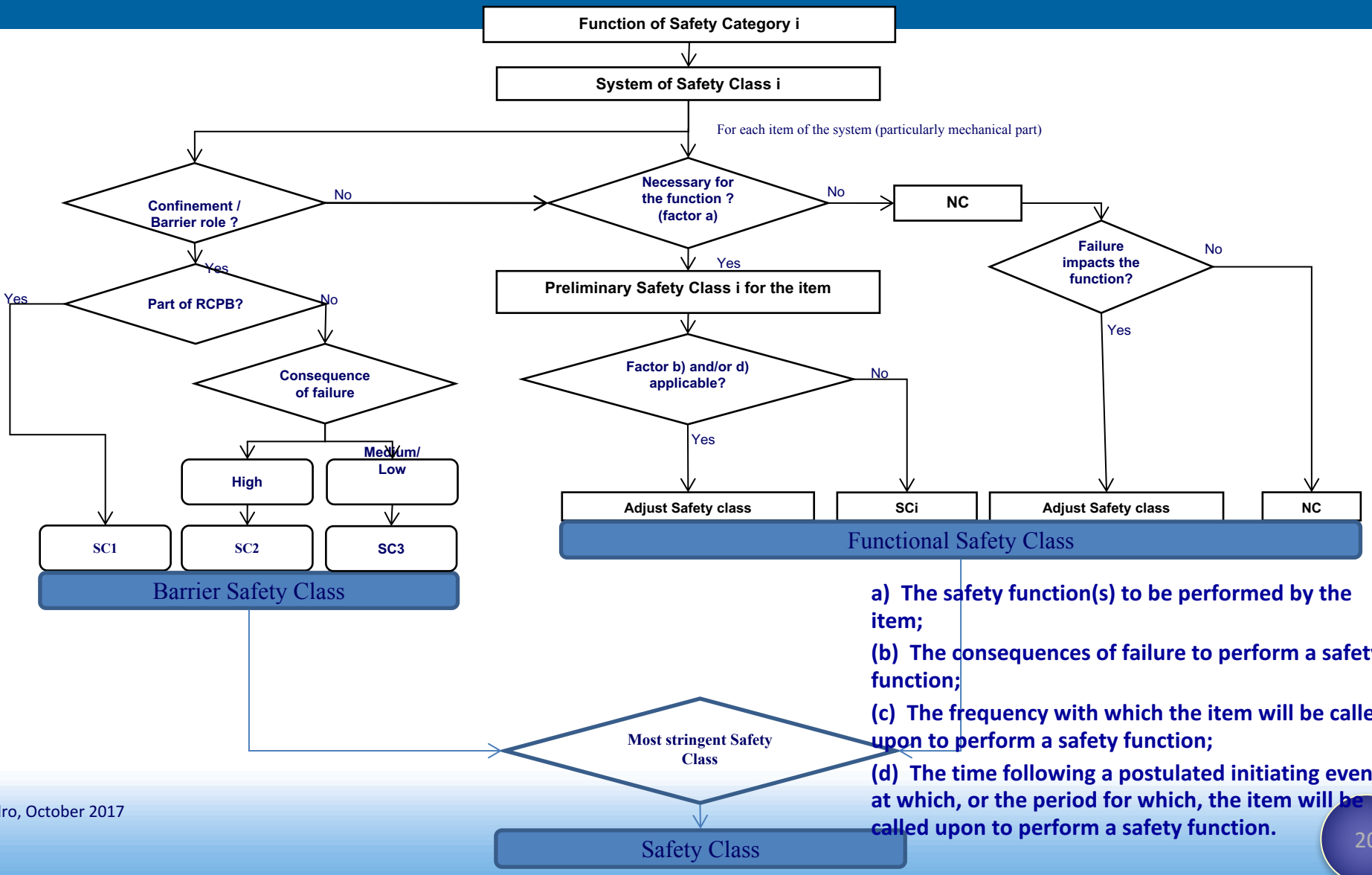
- **Any function relating to the monitoring needed to provide plant staff and off-site emergency services with a sufficient set of reliable information in the event of an accident (design basis accident or design extension conditions), including monitoring and communication means as part of the emergency response plan (defence in depth level 5), unless already assigned to a higher category.**

Classification of Structures, Systems and Components

Once the safety categorization of the functions is completed, the SSCs performing functions should be assigned to a safety class.

Systems are expected to be assigned to a safety corresponding to the safety category defined for the function performed.

Classification of Structures, Systems and Components



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

(b) The consequences of failure to perform a safety function;

(c) The frequency with which the item will be called upon to perform a safety function;

(d) The time following a postulated initiating event at which, or the period for which, the item will be called upon to perform a safety function.

Scope/ Design provisions

The safety of the plant is also dependent on the reliability of different equipment which, unlike to systems, is not called upon an event.

Design provisions are implemented to ensure that the main safety functions are fulfilled under modes of normal operation. Design provisions are mainly implemented for the following reasons:

- To protect people (workers and the public) and the environment from harmful effects of radiation (direct radiation, airborne activity and releases of radioactive material);
- To prevent the failure of an SSC not considered in the design basis for the plant (e.g. rupture of the reactor pressure vessel for LWR
- To reduce the frequency of failure of SSCs that may cause an accident;
- To limit the effects of hazards considered in the design basis for the plant;
- To prevent a postulated initiating event from developing into a more serious sequence without the occurrence of another independent failure.

Design provisions

- ***Design features that are designed to such a quality that their failure could be practically eliminated.*** *These design features can be readily identified by the unacceptable level of consequences that can be expected should they fail.*
E.g. Reactor pressure vessel

- ***Features that are designed to reduce the frequency of accident.***
E.g. piping of high quality whose failure would result in a design basis accident.

- ***Passive design features that are designed to protect workers and the public from harmful effects of radiation in normal operation.***
E.g. shielding, civil structures and piping.

- ***Passive design features that are designed to protect components important to safety from being damaged by internal or external hazards.***
E.g. concrete walls between components that are built specifically for this purpose.

- ***Features that are designed to prevent a postulated initiating event from developing into a more serious sequence.***
E.g. anti-whipping devices and fixed points.

Design provisions (cont'd)

- SSCs which might not be captured by the process of functional categorization and however which largely contribute to the safety, as for examples:.
  - Spent fuel storage racks contribute to the main safety function "Control of the reactivity
  - Reactor pressure vessel internals contribute to the main safety function "Heat removal",
  - Shielding to protect workers against radiation contributes to the main safety function "Confinement of radioactive material, shielding against radiation ".
- Mechanical components which contain radioactive materials and may lead to radiological consequences in case of failure (e.g. components of waste treatment systems, or components of systems controlling release of effluents.
- Buildings and civil structures.

Classification of Structures, Systems and Components (cont.)

In a single system, individuals components may have different safety classes depending on:

(a) The safety role performed by the component
(b) The consequences of its failure to perform the safety function;
(c) The frequency with which the item will be called upon to perform a safety function
(d) The time following a postulated initiating event at which, or the period for which, the item will be called upon to perform a safety function.

For individual components **containing radioactive materials** the consequences of their failure are identified with regards to the activity released and to the capability of the system to perform its intended function.

Classification of SSC

- Proposed classification includes 3 safety classes and 1 non safety class.
- SSC performing a function is generally classified consistently to the safety category of the function which it belongs.
- SSC / Design provision is generally directly classified taking into account the severity of consequence of its failure:

Class 1: Any SSC whose failure would directly lead, from normal operation, to a DEC or a BDBA, or result in consequences of 'high' severity,

Class 2: Any SSC whose failure, postulated from normal operation, would directly result in consequences of 'medium' severity,

Class 3: Any SSC whose failure, postulated from normal operation, would directly result in consequences of 'low' severity,

NC ; SSC not assigned in 1,2,3.

Safety class/ Engineering requirement

Safety Class	Safety classified pressure retaining equipment items	Example Codes	Example SSCs	Comments
Safety Class 1	• **Design provisions whose failure, in normal operation, would directly lead to ”high” consequences.**	ASME Code, Section III, Division 1, Subsection NB RCC-M1	Reactor pressure vessel, steam generator outer shells, piping to which leak-before-break or break preclusion principles are applied.	
	• **Any pressure retaining component which cannot be isolated from the reactor coolant system by two isolation valves in series and whose failure would result in leakage <u>not</u> compensable by the normal water make-up system (RCPB).**	ASME Code, Section III, Division 1, Subsection NB RCC-M1	RCPB piping > DN 25	Assigning the RCPB to the highest code requirements is not strictly required according to the SSG-30 definition of ‘high’ consequences (the deterministic safety analysis for loss of coolant accidents (LOCA) shall demonstrate that radiological consequences remain within acceptable limits). It is, however, common practice in many member states to strengthen DiD level 1 by choosing the highest quality requirements for the entire RCPB (except small-bore connecting lines).

Safety class/ Engineering requirement

Safety Class	Safety classified pressure retaining equipment items	Example Codes	Example SSCs	Comments
Safety Class 1	• **Components providing Cat. 1 functions unless codes like ASME Level 1 or RCC-M1 are already applied based on the rule above.**	ASME Code, Section III, Division 1, Subsection NC RCC-M2 RCC-M3 (see comment)	Emergency core cooling system, containment isolation system, reactor shutdown system.	Deviating from this general principle it is common practice in many member states to apply codes likes ASME Level 3 or RCC-M3 if these class 1 components are, in normal operation, • subject of small service loads (moderate operating pressure and temperature) AND • do not contain high radioactive fluids. Examples: Service water pump system, auxiliary feedwater system portions isolated from steam generator pressure and temperature.

Safety class/ Engineering requirement

Safety Class	Safety classified pressure retaining equipment items	Example Codes	Example SSCs	Comments
Safety Class 2	• **Safety class 2 design provisions whose failure, in normal operation, would directly lead to ‚medium' consequences.** • **Any parts of the RCPB whose failure would result in leakage compensable by the normal water make-up system.** • **Components providing Cat. 3 functions with a safety barrier class 2**	ASME Code, Section III, Division 1, Subsection NC RCC-M2	Residual heat removal system. Non-isolable primary piping < DN25.	The residual heat removal system performs a Cat. 2 function but recirculates primary water in normal shutdown operation and provides therefore also an important barrier role (‘medium’ consequences in case of pipe failure).
	• **Components providing Cat. 2 functions**	ASME Code, Section III, Division 1, Subsection ND RCC-M3	Spent fuel pool cooling system.	

Safety class/ Engineering requirement

Safety Class	Safety classified pressure retaining equipment items	Example Codes	Example SSCs	Comments
Safety Class 3	• **Safety class 3 design provisions whose failure, in normal operation, would directly lead to ‚low' consequences.** • **Components providing Cat. 3 functions with a safety barrier class 3.**	ASME Code, Section III, Division 1, Subsection ND RCC-M3	Systems containing radioactive fluids in normal operation, e.g. chemical volume and control system, waste processing systems.	
	• **Components providing Cat. 3 functions unless specific codes and requirements are applied for specific reasons.**	Conventional codes like • European Pressure Directive 97/23/EC. • ASME Code, Section VIII, Division 1 for pressure vessels, • ASME B31.1 for piping.	Systems providing make-up to feedwater tanks in postulated design extension conditions.	Systems providing functions for severe accident management on DiD level 4 should be subject of specific requirements reflecting the role and the environmental conditions of the components in postulated severe accident scenarios. Guidance from codes like ASME or RCCM should be taken where appropriate. As an example ASME Level 2 or RCC-M2 may be applied for pressure retaining parts extending the primary containment in case of severe accidents.

Verification of the safety classification

- Comparison of the classification established according to a the deterministic approach (e.g. application of the IAEA SSG-30) with insights from probabilistic safety assessment
- Expectation:
  - Consistency between the deterministic and probabilistic approaches provides confidence that the safety classification is correct
  - If there are differences further assessment should be carried out in order to understand the reasons for these and a final safety class should be assigned
- Iterative process to ensure the completeness of the classification

Selection of engineering design rules for SSCs

- Three characteristics of the engineering design rules:
  - **Capability**
  - **Dependability**
  - **Robustness**

A complete set of engineering design rules should be specified to ensure that the safety classified SSCs will be designed, manufactured, constructed, installed, commissioned, operated, tested, inspected and maintained to appropriate and well proven quality standards.

Engineering requirements give confidence that reliability of every SSC is commensurate to their individual safety significance.

Selection of engineering design rules for SSCs

To achieve the expected reliability:

- At the system level, design requirements to be applied may include specific requirements, such as single failure criteria, independence of redundancies, diversity and testability.
- For individual structures and components, design requirements to be applied may include specific requirements such as environmental and seismic qualification, and manufacturing quality assurance procedures. They are typically expressed by specifying the codes or standards that apply.
- Appropriate codes and standards(for pressure retaining equipment: ASME, RCC-M, etc., for I&C IEC or IEEE, etc.) and clear links between safety classes and code acceptance criteria
- Regulatory limits and acceptance criteria

…Thank you for your attention

Safety class/ Engineering requirement

Electrical equipment includes various types of equipment like AC and DC power sources, transformers, switchgears, electrical distribution system, protection devices, etc.

Safety Class	Safety classified electrical equipment items	Examples of Code	Example SSCs	Comments
1	• **Electrical equipment supporting Cat. 1 or functions**	IEEE: 1E RCC-E: EE1	On site AC power supply system, uninterruptible DC power supply system	
2	• **Electrical equipment supporting Cat. 2 functions in DBAs**	IEEE: 1E RCC-E: EE1	Electric drives supporting Cat. 2 functions.	
	• **Electrical equipment supporting Cat. 2 functions implemented as a back-up for a Cat. 1 function**	RCC-E: EE1 IEEE: Specific requirements	Electric drives supporting back up of Cat. 2 functions.	The IEEE codes don't stipulate explicit requirements for equipment used in design extension conditions without core melt. Additional specific requirements are typically defined.
3	• **Electrical equipment supporting Cat. 3 functions**	IEEE: non 1E RCC-E: EE2 + specific requirements	Alternate AC power sources Uninterruptable power supply system for severe accidents Electric drives supporting Cat. 3 functions.	Equipment used in severe accident shall be qualified for the harsh environmental condition resulting from severe accidents.