Joint ICTP-IAEA Essential Knowledge Workshop on Deterministic Safety Analysis and Engineering Aspects Important to Safety

Trieste,12-23 October 2015

Safety classification of structures, systems and components

Marco Gasparini / Bernard Poulat
IAEA

IAEA
International Atomic Energy Agency

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

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 has tried to provide a rational for the creation of a classification scheme to comply with the requirements established in SSR-2/1.
-

IAEA

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.

IAEA

General approach

Requirement 4: Fundamental Safety Functions

Fulfilment of the following fundmental safety functions shall be ensured for all plant states:

(i) control of reactivity,

(ii) removal of heat from the reactor and from the fuel store and

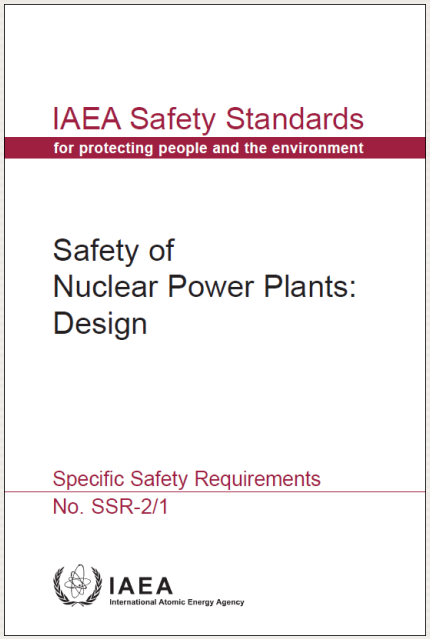
(iii) confinement of radioactive material, shielding against radiation and control of planned radioactive releases, as well as limitation of accidental radioactive releases.

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.

IAEA

General approach



5.34. 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.

IAEA

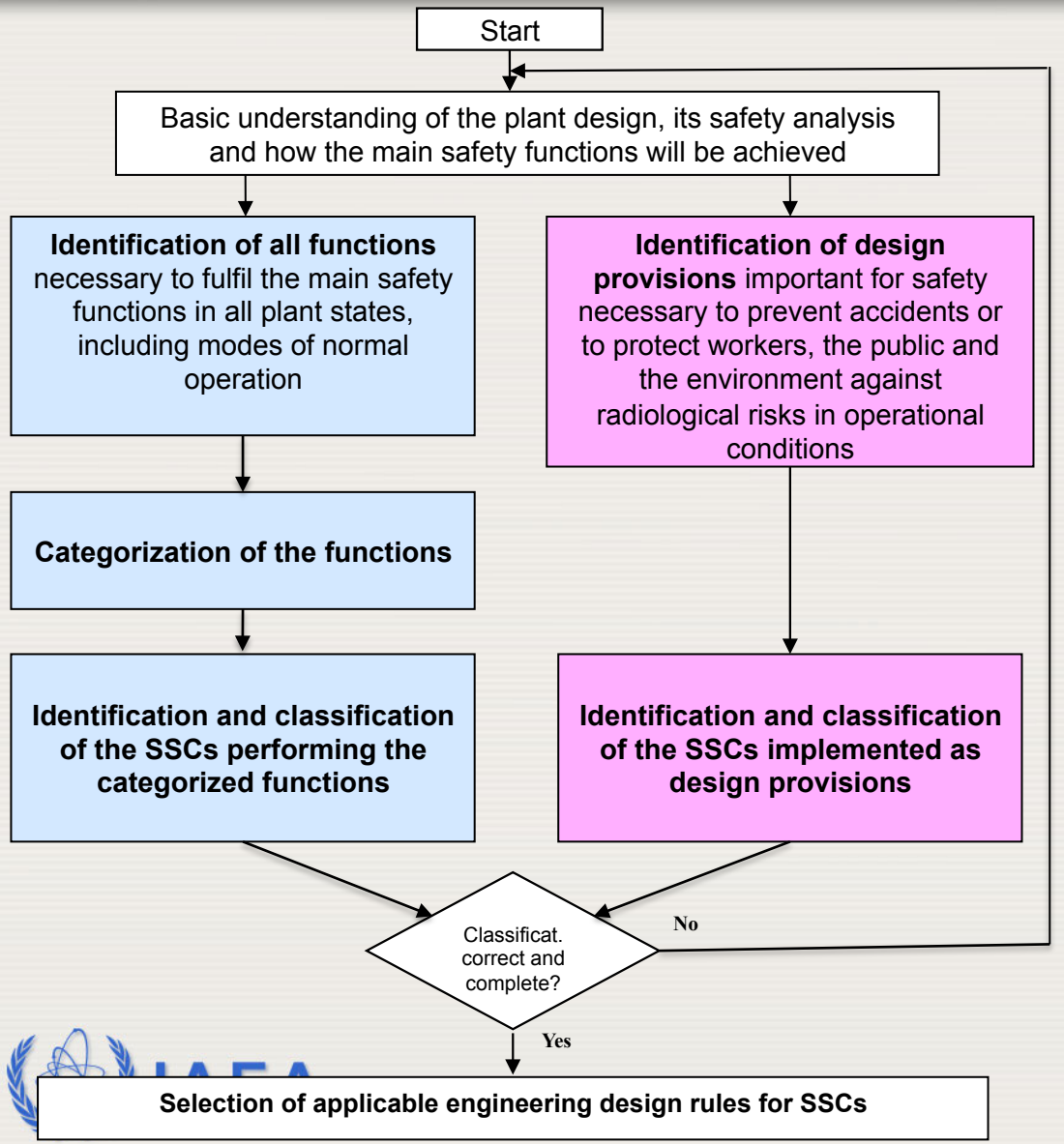
Pre-requisites to Safety classification

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

IAEA

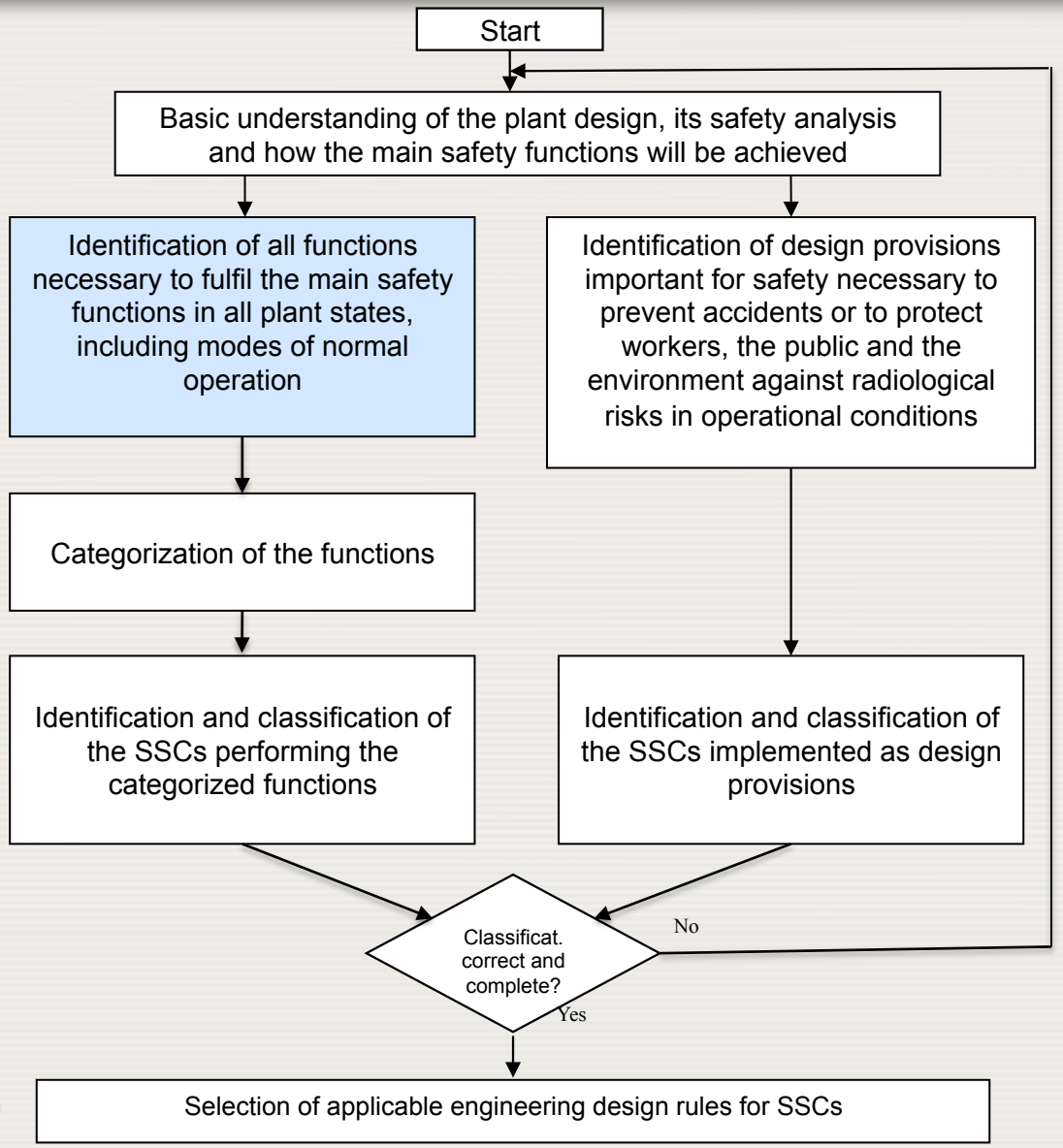
Classification process



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

Identification of safety functions



IAEA

Identification of safety functions

- Safety functions to be identified are those required to achieve the fundamental 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 fundamental safety functions to be fulfilled are the same for every plant state, more specific safety functions should be identified for each plant state.

- It is recommended to detail functions as needed to cover all actions to be accomplished by the systems in the different plant states. The number of functions is usually small for a conceptual design but it is growing while the design is developing.

IAEA

Identification of safety functions

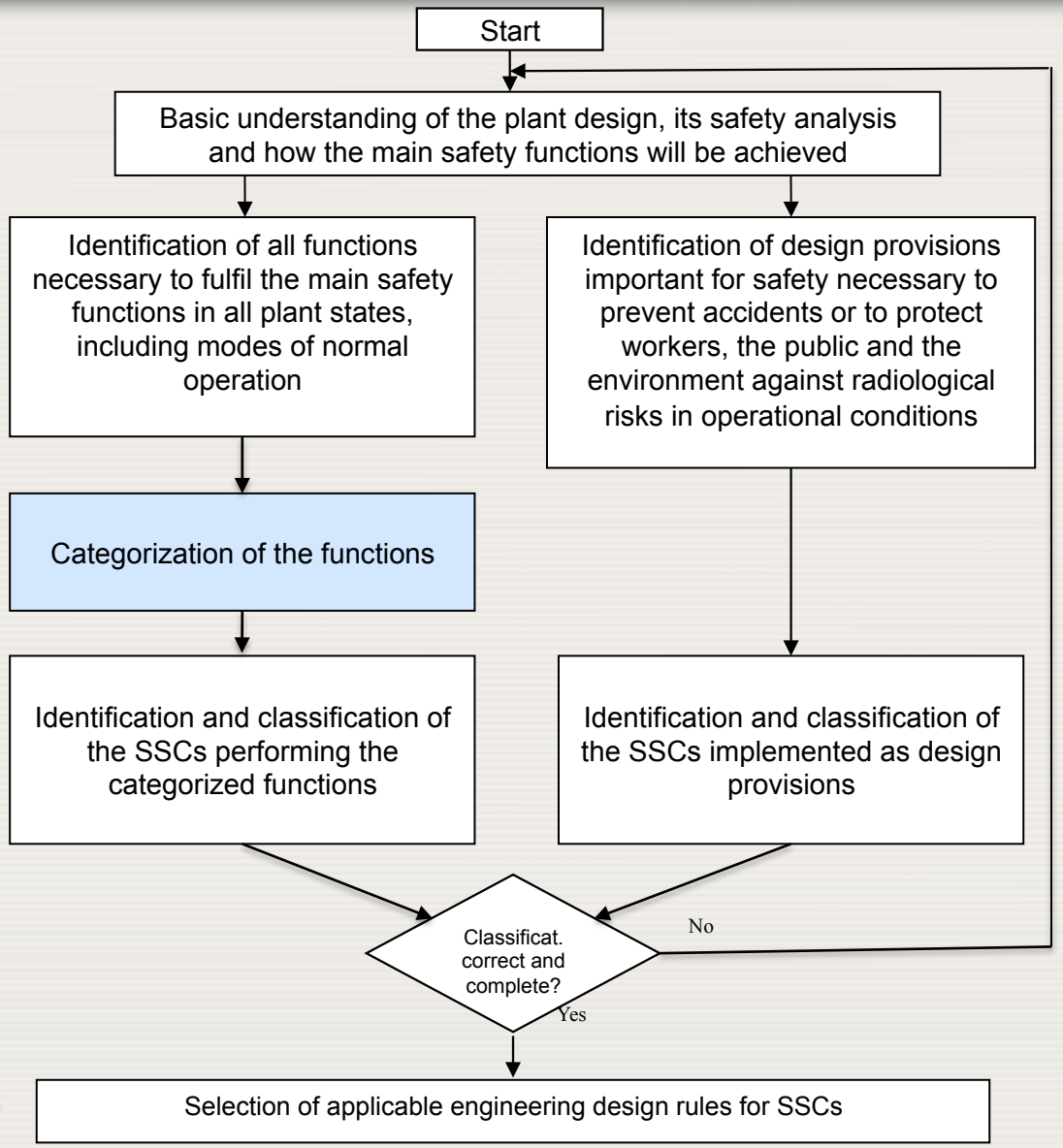
Fundamental Safety Function	Functions to be categorized for the different plant states
Control of Reactivity	R1 - Maintain core criticality control
	R2 - Shutdown and maintain core sub-criticality
	R3 - Prevention of uncontrolled positive reactivity insertion into the core
	R4 - Maintain sufficient sub-criticality 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

Identification of safety functions

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

IAEA

Categorization of safety functions



IAEA

Categorization of functions

- The categorization of functions is a process which is system independent (technology neutral).
- For each PIE, the functions necessary to control or mitigate the consequences are identified and categorized.
- The categorization of functions is performed to reflect the safety significance of each function.
- Safety significance is assessed taking into account 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.

IAEA

Severity of consequences

Severity of consequences	Consequences of the failure of the functions
High	• Lead to a release of radioactive material that exceeds the limits accepted by the regulatory body for design basis accidents; or • Cause the values of key physical parameters to exceed acceptance criteria for design basis accidents
Medium	• Lead to a release of radioactive material that exceeds limits established for anticipated operational occurrences; or • Cause the values of key physical parameters to exceed the design limits for anticipated operational occurrences
Low	• Lead to doses to workers above authorized limits

IAEA

Criteria for categorization of functions

Safety category 1	Examples
Any function required to reach the controlled state after an AOO or a DBA and whose failure, when challenged, would result in consequences of 'high' severity.	Automatic and fast reactor trip; Core cooling for Design basis accident.
Safety category 2	
Any function required to reach the controlled state after an AOO or a DBA and whose failure, when challenged, would result in consequences of 'medium' severity;	Functions associated with limiting off-site releases in DBAs (e.g. filtered HVAC) provided their failure would not directly lead to releases above authorized limits;
Any function required to reach and maintain a safe state for a long time and whose failure, when challenged, would result in consequences of 'high' severity;	Residual heat removal in the long term;
Any function designed to provide a backup of a function categorized in safety category 1 and required to control DEC without core melt.	Diverse actuation trip function as a backup of the reactor trip function.
Safety category 3	
Any function actuated in the event of an AOO or DBA and whose failure when challenged would result in consequences of 'low' severity;	Functions designed to prevent the use of safety systems in AOOs (e.g. normal and auxiliary pressurizer spray);
Any function required to reach and maintain a safe state for a long time and whose failure, when challenged, would result in consequences of 'medium' severity;	Service water filtration (if necessary in the longer term).
Any function required to mitigate the consequences of DEC, unless already required to be categorized in safety category 2, and whose failure, when challenged, would result in consequences of 'high' severity;	Containment heat removal in case of a severe accident;

Categorization of functions

Safety category 3 (cont.)

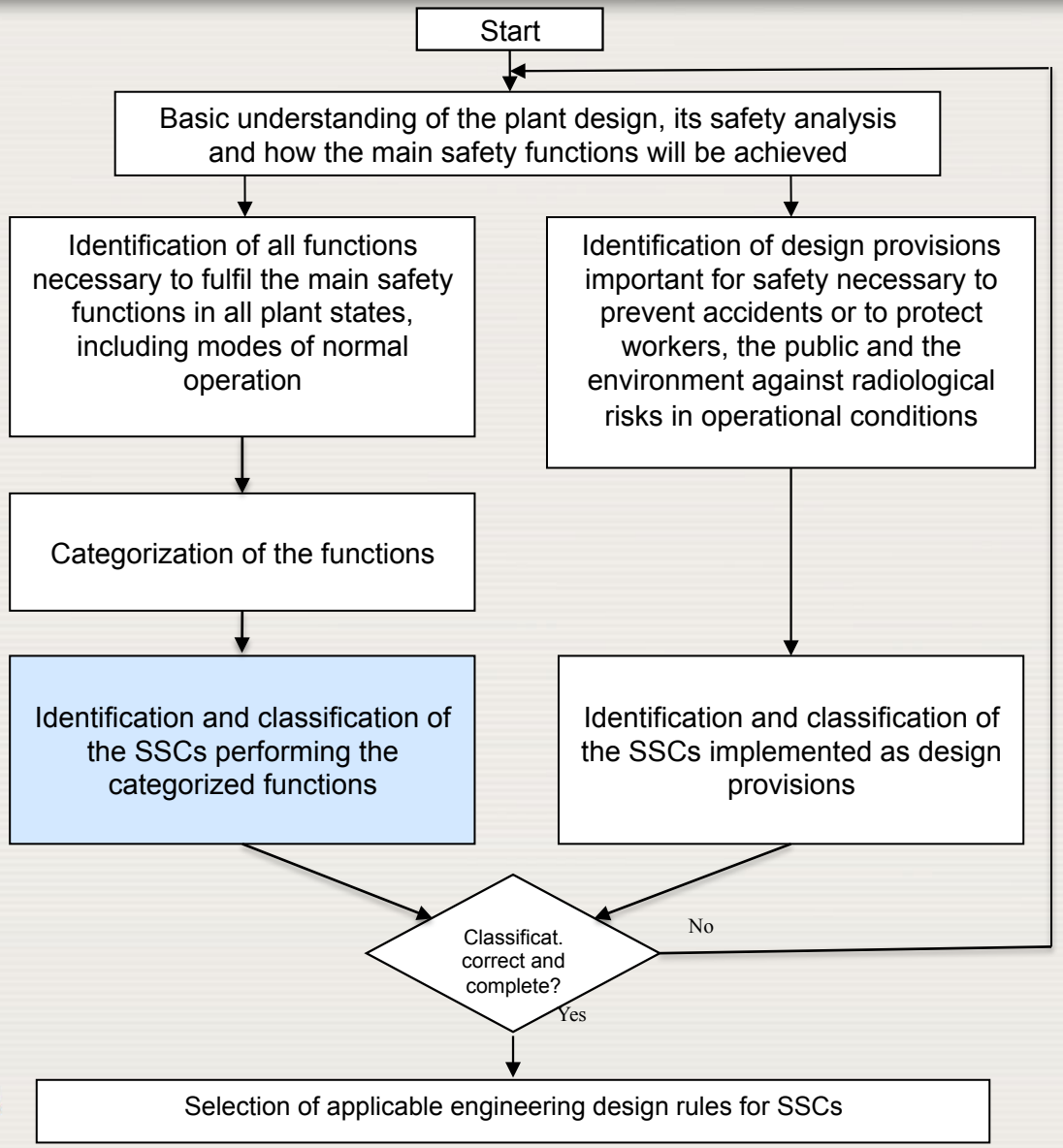
Any function designed to reduce the actuation frequency of the reactor trip or engineered safety features in the event of a deviation from normal operation, including those designed to maintain the main plant parameters within the normal range of operation of the plant;	The reactor power control in an AOO to avoid emergency shutdown; Control the water level of the pressurizer by normal charge or letdown flowrate to avoid safety inject; Control the pressure of the pressurizer by spray and heater to avoid opening the safety release valve of the pressurizer; Control the water level of the SG by normal feedwater to avoid auxiliary feedwater run; Control the pressure of the SG by the steam turbine bypass system to avoid opening the main steam safety valve;
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 (DBAs or DEC), including monitoring and communication means as part of the emergency response plan (DID level 5), unless already assigned to a higher category.	Emergency feedwater tank level monitoring; Safety injection tank pressure detection; Emergency communication, emergency lighting function;
The function which is used for limiting the effects of internal/external hazards.	Fire extinguishing; fire containing by closure of fire dampers on demand of a fire detection system.

Relation between functions and safety categories

Functions credited in the safety assessment	Severity of the consequences if the function is not performed		
	High	Medium	Low
Functions to reach a controlled state after AOOs	Safety category 1	Safety category 2	Safety category 3
Functions to reach a controlled state after DBAs	Safety category 1	Safety category 2	Safety category 3
Functions to reach and maintain a safe state	Safety category 2	Safety category 3	Safety category 3
Functions for the mitigation of consequences of DECs	Safety category 2 or 3	Not categorized	Not categorized

IAEA

Identification of safety functions



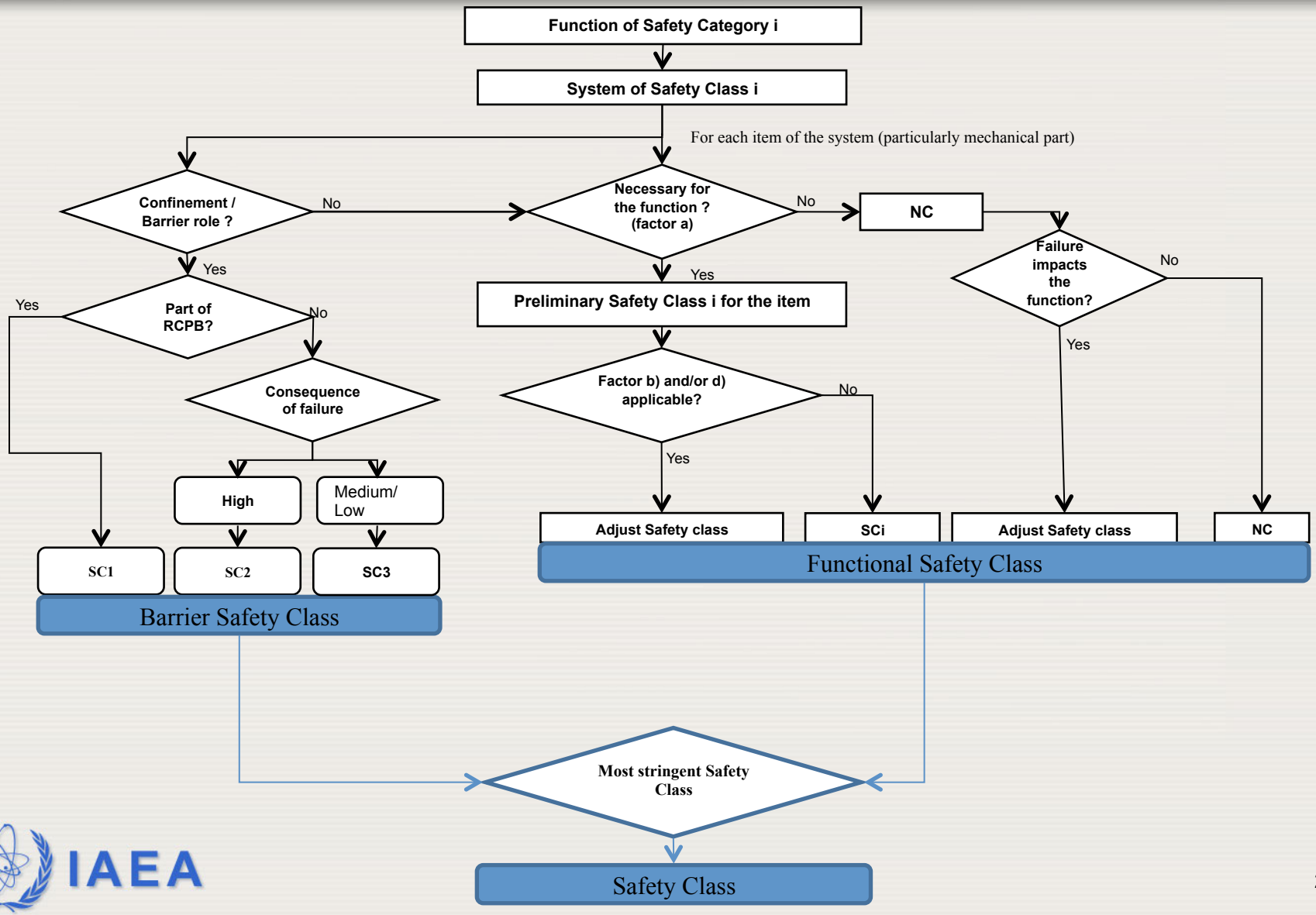
IAEA

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 class corresponding to the safety category defined for the function performed.

Classification of Structures, Systems and Components

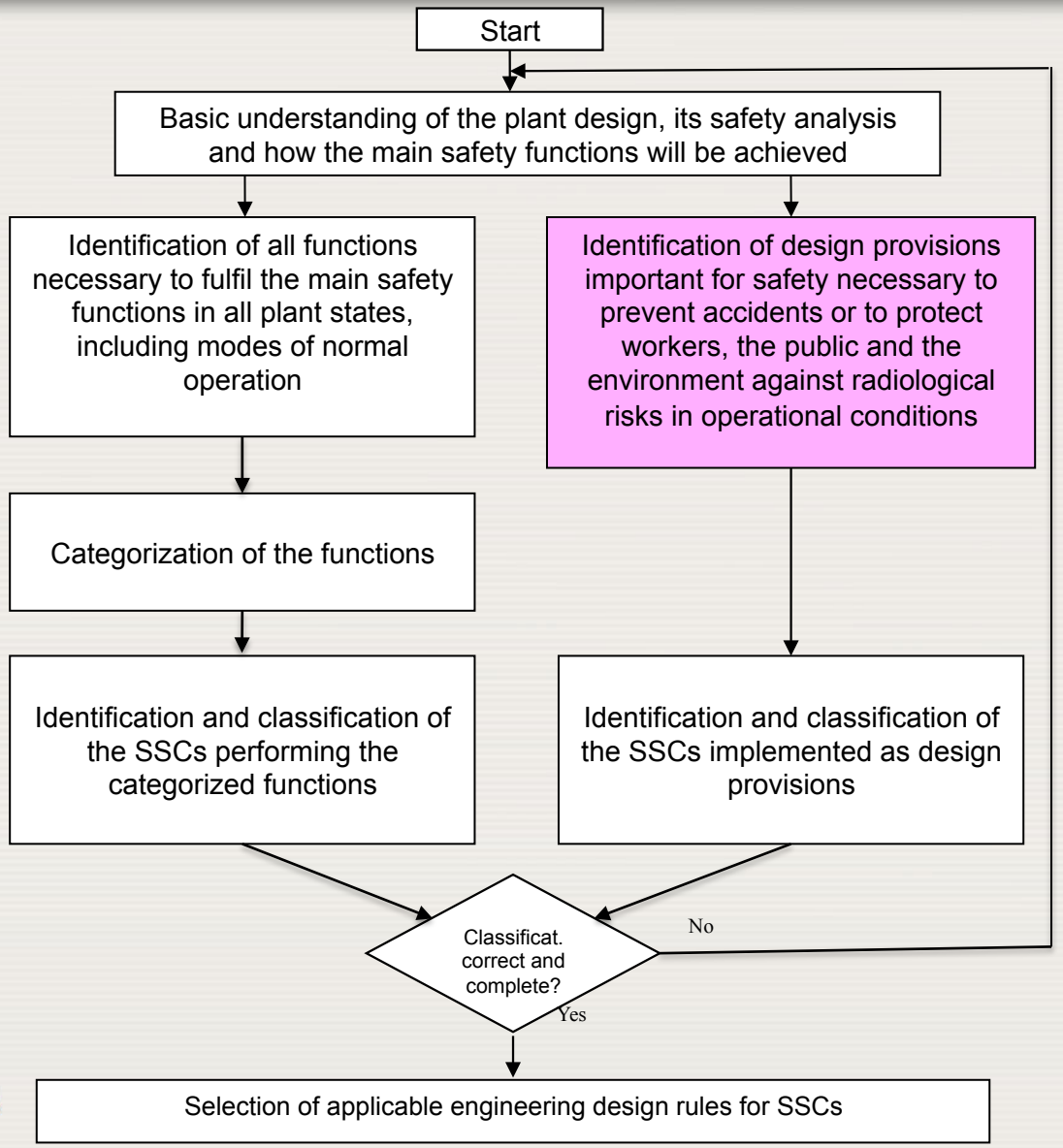


Engineering rules for systems

Function	Category of function	Safety class of system performing the function	Redundancy requirement	Independence of redundant trains	Physical separation of redundant trains	Periodic testing	Qualification to environmental conditions	Quality assurance
Emergency core Cooling	Cat. 1	Class 1	Yes	Yes	Yes	Yes	Harsh or mild, depending on system location.	Nuclear grade
Long term residual heat removal (beyond the function of the emergency core cooling system)	Cat. 2	Class 2	Yes	Yes	Yes	Yes	Harsh or mild, depending on system location.	Nuclear grade or specific requirements
Containment depressurization after a severe accident	Cat. 3	Class 3	Not strictly required but widely implemented	No	No	Yes	Severe accident conditions	Specific requirements
Functions to warn personnel about the risk of radiation exposure beyond the acceptable limits	Cat. 3	Class 3	No	No	No	Yes	No	Commercial grade or specific requirements

IAEA

Identification of design provisions



IAEA

Identification of design provisions

The safety of the plant is also dependent on the reliability of different types of features, some of which are designed specifically for use in normal operation.

In the Safety Guide SSG-30, these SSCs are termed **'design provisions'**.

Design provisions should be identified and may be considered to be subject to the safety classification process, and hence will be designed, manufactured, constructed, installed, commissioned, operated, tested, inspected and maintained with sufficient quality to fulfil their intended role.

IAEA

Identification of 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.
Example: **Reactor pressure vessel**

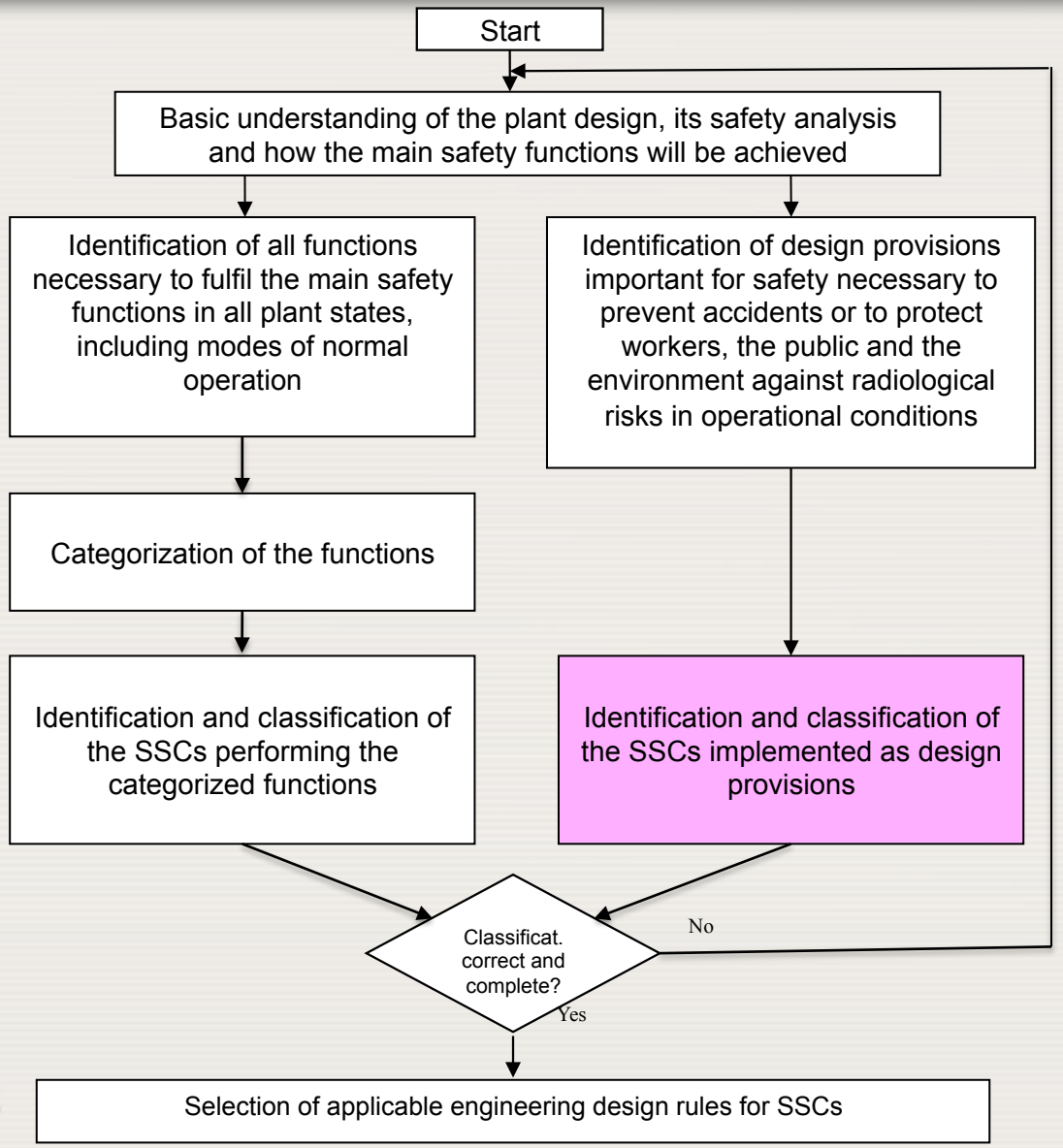
• Features that are designed to reduce the frequency of accident.
Example: **piping of high quality whose failure would result in a design basis accident**.

• Passive design features that are designed to protect workers and the public from harmful effects of radiation in normal operation.
Example: **shieldings, civil structures and piping**.

• Passive design features that are designed to protect components important to safety from being damaged by internal or external hazards.
Example: **concrete walls between components**

• Features that are designed to prevent a postulated initiating event from developing into a more serious sequence.
Example: **anti-whipping devices and fixed point**s.

Identification of safety functions



IAEA

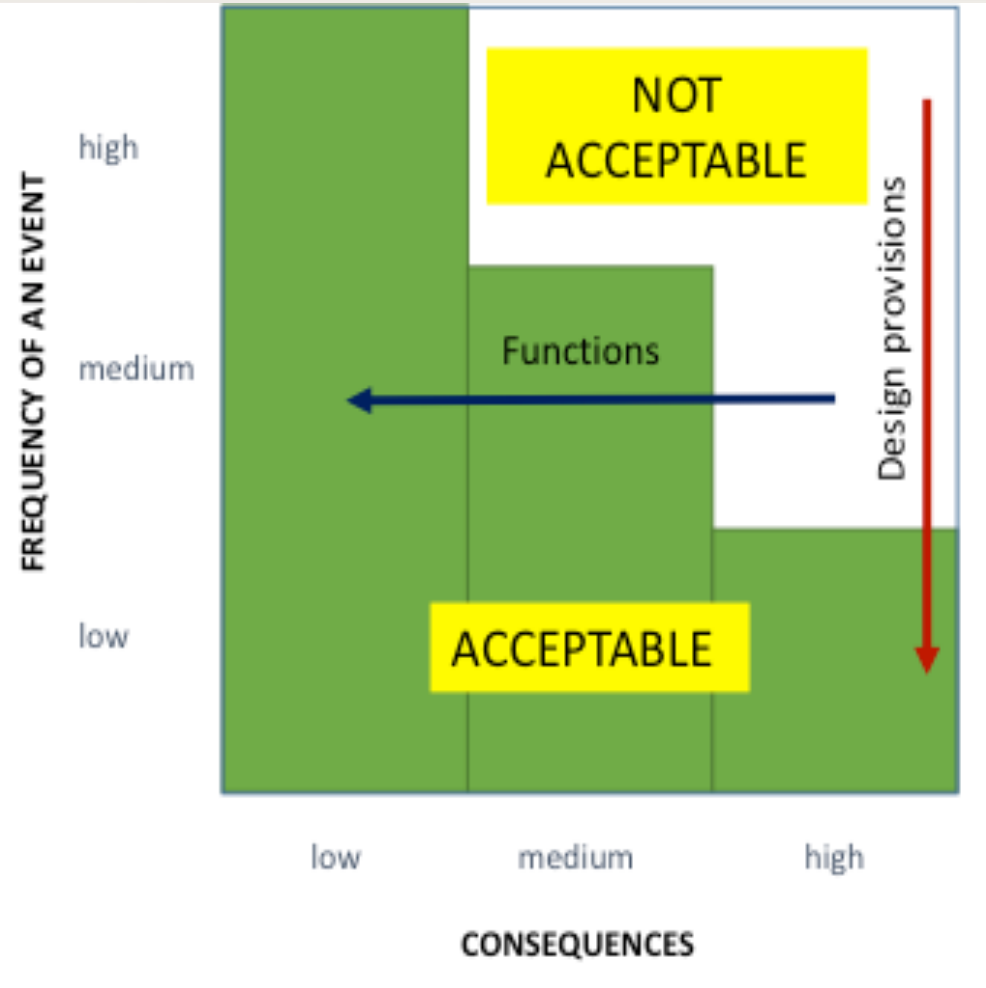
Classification of Design provisions

- Design provision is generally directly classified taking into account the severity of consequence of its failure:
    - Safety class 1: Any SSC whose failure would directly lead to consequences of ‘high’ severity,
    - Safety class 2: Any SSC whose failure would lead to consequences of ‘medium’ severity,
    - Safety class 3: Any SSC whose failure would lead to consequences of ‘low’ severity,
    - NC ;SSC not assigned in 1,2,3.

IAEA

Event frequency versus consequences

A correct classification process would result in a balanced risk (events with a high level of severity of consequences have a very low predicted frequency of occurrence)



IAEA

Selection of engineering design rules for SSCs

- 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.
- These rules are normally included in national or international codes, standards and proven engineering practices that should be applied.
- The correct application of national and international codes guarantees that the needed capability, reliability and robustness of SSCs are achieved

IAEA

Selection of engineering design rules for SSCs

Design requirements for systems and for individual structures and components:

- 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

Examples of safety classes and codes

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).

Examples of safety classes and codes

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.

IAEA

Examples of safety classes and codes

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.	

Examples of safety classes and codes

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 RCC-M 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.

Examples of safety classes and codes

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.

...Thank you for your attention

IAEA