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

Trieste,12-23 October 2015

Safety Design Requirements

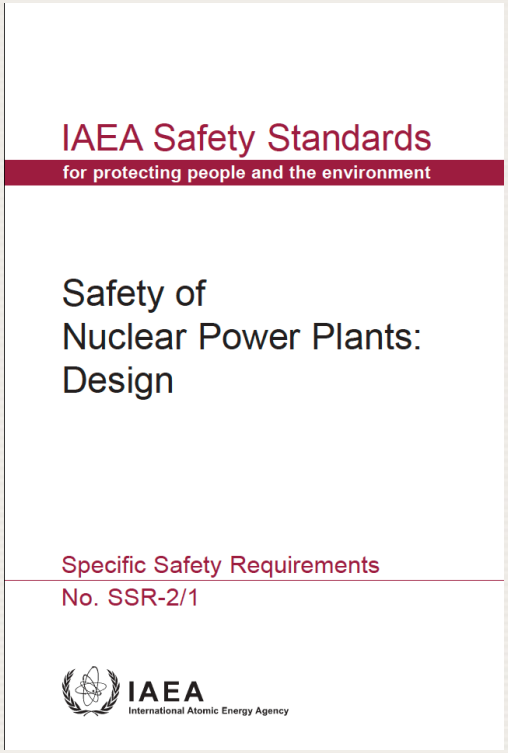
Overview of SSR-2/1

Marco GASPARINI
(IAEA Consultant)

IAEA
International Atomic Energy Agency

Requirements for design of NPPs

To be implemented by the designer to fulfill the fundamental safety functions with the appropriate level of defence in depth



To be used by the reviewer of the design (e.g. Safety Authority) to assess the safety of the design

SSR-2/1 (revision of NS-R-1) has been published on 20 Feb 2012

IAEA

Note by the Secretariat

(…)

The present publication reflects feedback and experience accumulated until 2010 and it has been subject to the rigorous review process for standards.

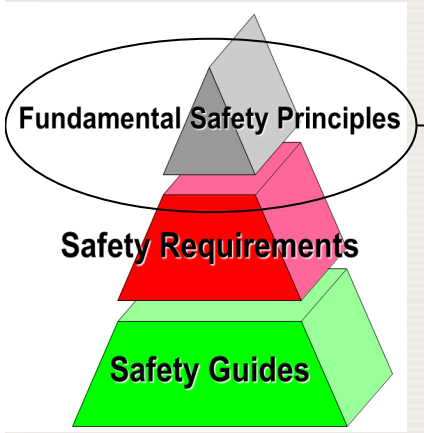
A task to include the lessons learned from the Fukushima's accident in SSR-2/1 has been completed. SSR-2/1 Rev 1 has been approved by the Board of Governors of the IAEA and is in printing

IAEA

IAEA Fundamental Safety Principles (2006)

Safety Objective

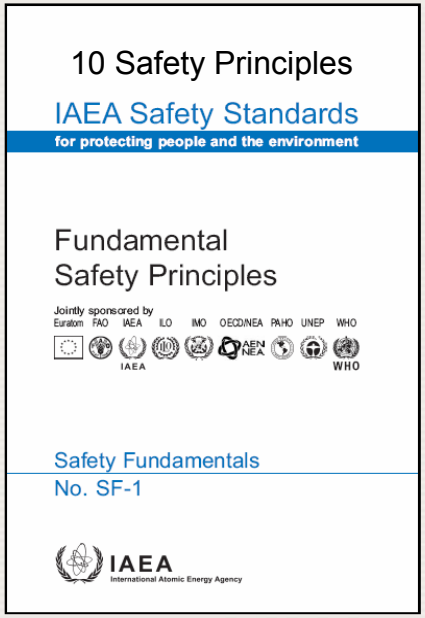
To protect people and the environment from harmful effects of ionizing radiation



Responsibility for Safety

Role of Government

Leadership and Management for Safety



Protective Actions to Reduce Existing Or Unregulated Radiation Risks

Emergency Preparedness and Response

Prevention of Accidents

Justification of Facilities and Activities

Optimization of Protection

Limitation of Risks to Individuals

Protection of Present and Future Generations

IAEA

Three Fundamental Safety Functions

Under all circumstances

(normal operating conditions as well as in incident and accident conditions)

it is necessary to

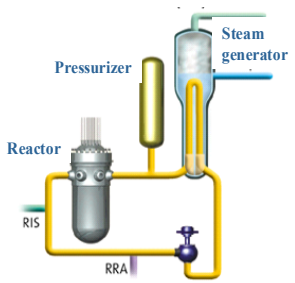
Control the reactivity

- control rods
- boron concentration

Remove the heat from the fuel

Heat removal :

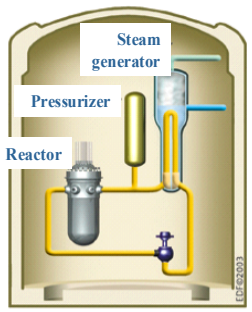
- by steam generators in operation
- by residual heat removal
- by safety injection



Confine the radioactive material

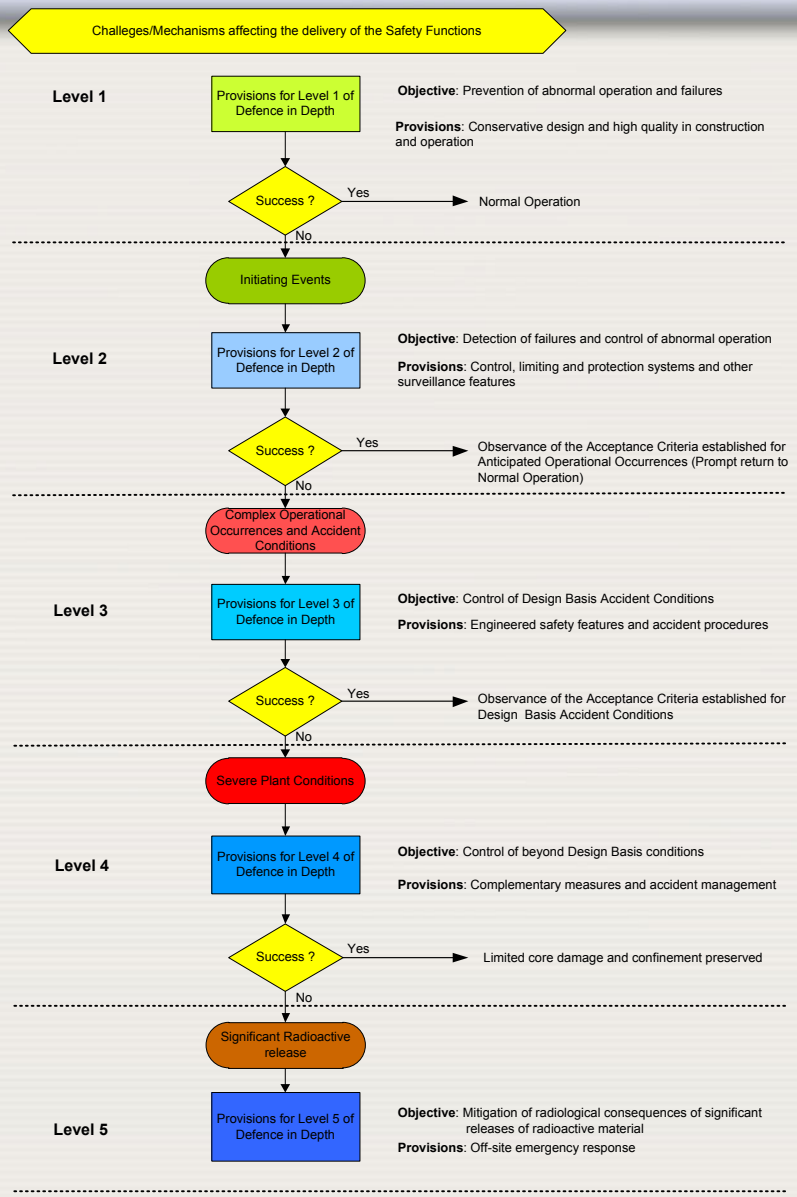
By the 3 barriers :

- fuel cladding
- primary cooling system
- containment building



IAEA

Flow Diagram of Defence in Depth



Effective implementation of Defence in Depth requires (at all levels):

- Conservatism
- Quality assurance
- Safety Culture

Plant states

Normal Operation

Anticipated Operational Occurrences

Accidents (DBA)

Design Extension Conditions (DECs)

IAEA

Main Pillars for a safe NPP design

Fundamental Safety Principles

-Safety Objective

-Safety principles

-

- Principle of prevention of accidents

-

-

Fundamental Safety Functions

- Control of reactivity
- Removal of heat from the fuel
- Confinement of radioactive material and shielding against radiation

Defence in depth

Effective strategy in compensating for human errors and equipment failures

Based on several levels of protection and physical barriers preventing the release of radioactive material to the environment

IAEA

Importance of the Requirements for the Design of NPPs

- Define an effective safety approach and establish the safety "**level**" for designs of nuclear power plants
  - reflect the state of the art
  - reflect the views and the licensing practices of the majority of IAEA Member States
  - reflect a large consensus
- Provide links with the requirements for site evaluation and for operation
  - taking into consideration the impact of the site on the design
  - providing for easy and safe operation over the lifetime of the plant

IAEA

Importance of the Requirements for the Design of NPPs

- are the main reference to perform IAEA design safety reviews
  - basis for the preparation of guidelines to conduct design safety reviews
  - basis for the safety assessment
- significantly contribute to establishing a common safety approach and common terminology
- used as reference for establishing licensing regulations in several countries
  - in some cases adopted as national regulation
  - In some cases used to integrate existing national regulations

IAEA

Contents of the former NPP Design Requirements (N-SR-1)

- INTRODUCTION
- SAFETY OBJECTIVES AND CONCEPTS

} SAFETY OBJECTIVES DEFENCE IN DEPTH

- REQUIREMENTS FOR MANAGEMENT OF SAFETY
- PRINCIPAL TECHNICAL REQUIREMENTS
- REQUIREMENTS FOR PLANT DESIGN
- REQUIREMENTS FOR DESIGN OF PLANT SYSTEMS

} 208 REQUIREMENTS ("SHALL" STATEMENTS)

- APPENDIX ON PIEs
- ANNEX ON REDUNDANCY, DIVERSITY AND INDEPENDENCE
- ANNEX ON SAFETY FUNCTIONS FOR WATER COOLED REACTORS

} SUPPORTING INFORMATION AND EXPLANATIONS

IAEA

Major changes in SSR 2/1 w.r.t. NS-R-1

- **General improvement of the text and elimination of repetitions**
- **New style of format for Safety Requirements**
- **Emphasis on independence of levels of defence in depth**
- **Requirement on interfaces between safety, security and safeguards**
- **Requirement on Safety of the design throughout the plant life**
- **Requirements on auxiliary and supporting systems**
- **More detailed description of the conditions to be considered in the design of SSCs (Design basis)**
- **New definitions**
  - Design extension conditions, DECs
  - Safe state, Controlled state
- **Revised Definitions**
  - Accident conditions
  - Design basis accidents
- **Explicit distinction between "Safety Systems" and "Safety Features for DECs"**
- **Qualitative acceptable radiological consequences for "Accident Conditions"**

IAEA

Structure of SSR 2/1

- **Sections 1-2 :** Introduction, Principles and concepts

- **Section 3 :** Requirements on management of safety in design

- **Sections 4- 5 :** Requirements applicable to all SSCs important to safety

- **Section 6:** Requirements for specific plant systems

  Reactor core, Reactor coolant systems, Containment systems, I&C, Emergency power supply, Radioactive effluents treatment, Fuel handling and storage systems

IAEA

Defence in depth in NS-R-1 and SSR-2/1

INSAG-10/NS-R-1

Levels of defence	Objective	Essential means
Level 1	Prevention of abnormal operation and failures	Conservative design and high quality in construction and operation
Level 2	Control of abnormal operation and detection of failures	Control, limiting and protection systems and other surveillance features
Level 3	Control of accidents within the design basis	Engineered safety features and accident procedures
Level 4	Control of severe plant conditions, including prevention of accident progression and mitigation of the consequences of severe accidents	Complementary measures and accident management
Level 5	Mitigation of radiological consequences of significant releases of radioactive materials	Off-site emergency response

SSR-2/1

Level of defence (Option 1)	Objective	Essential means	Level of defence (Option 2)
Level 1	Prevention of abnormal operation and failures	Conservative design and high quality in construction and operation	Level 1
Level 2	Control of abnormal operation and detection of failures	Control, limiting and protection systems and other surveillance features	Level 2
Level 3 (3a)	Control of design basis accidents (postulated single initiating events)	Engineered safety features (safety systems) and accident procedures	Level 3
Level 3 (3b)	**Control of design extension conditions to prevent core melt**	**Safety features for design extension conditions without core melt; emergency operating procedures**	4a
Level 4	Control of design extension conditions to mitigate the consequences of severe accidents	Safety features for design extension conditions with core melt. Complementary emergency procedures. SAM guidelines	Level 4 4b
Level 5	Mitigation of radiological consequences of significant releases of radioactive materials	On-site and off-site emergency response facilities	Level 5

IAEA

Contents of the NPP Design Requirements (SSR 2/1)

- INTRODUCTION
- APPLYING SAFETY PRINCIPLES AND CONCEPTS

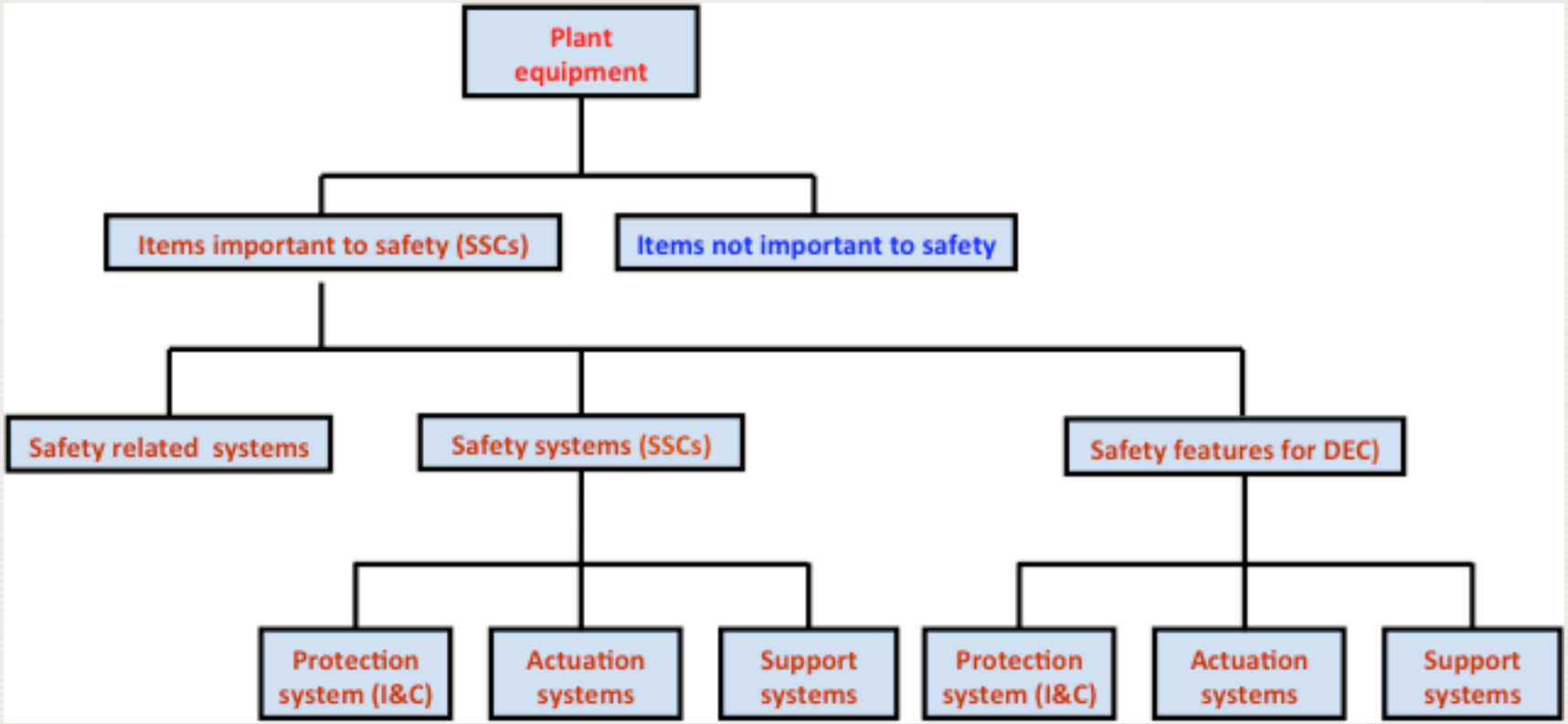
Safety objectives; Radiation protection; Defence in depth

- MANAGEMENT OF SAFETY IN DESIGN
  - 3 Requirements
- PRINCIPAL TECHNICAL REQUIREMENTS
  - 9 Requirements
- GENERAL PLANT DESIGN
  - Design Basis (16 Requirements)
  - Safe Operation Over Lifetime of Plant (3 Requirements)
  - Human Factors (1 Requirement)
  - Other Design Considerations (9 Requirements)
  - Safety Analysis (1 Requirement)
- DESIGN OF SPECIFIC PLANT SYSTEMS
  - Reactor Core and Associated Features (4 Requirements)
  - Reactor Coolant Systems (7 Requirements)
  - Containment Structure and Containment System (5 Requirements)
  - Instrumentation and Control Systems (9 Requirements)
  - Emergency Power Supply (1 Requirement)
  - Supporting Systems and Auxiliary Systems (8 Requirements)
  - Other Power Conversion Systems (1 Requirement)
  - Treatment of Radiological Effluents and Radioactive Waste (2 Requirements)
  - Fuel Handling and Storage System (1 Requirement)
  - Radiation Protection (2 Requirements)

82 KEY REQUIREMENTS
186 Supporting Requirements
("SHALL" STATEMENTS)

IAEA

Plant equipment



IAEA

Plant states considered in the design

Plant states considered in the design				
Operational states		Accident conditions		
Normal operation (NO)	Anticipated operational occurrences (AOO)	Design basis accidents (DBA)	Design extension conditions (DEC)	
			without significant fuel degradation	with core melt

Plant state	Indicative expected frequency of occurrence (*)
Normal operation	**-**
Anticipated operational occurrences	**> 10^{-2} events per year**
Design basis accidents	**10^{-2} – 10^{-6} events per year**
Design extension conditions without significant fuel degradation	**10^{-4} – 10^{-6} events per year**
Design extension conditions with core melt	**< 10^{-6} events per year**

IAEA

(*) These values are indicative and they are not specified in SSR-2/1

SSR-2/1 versus NS-R-1, plant states

NS-R-1, 2000

Operational states		Accident conditions		
NO	AOO	(a)	DBAs	(Beyond design basis accidents)
				(b) Severe Accidents
1st level DiD	2nd level DiD	3rd level DiD		4th level DiD
Included in the design basis				Beyond design basis

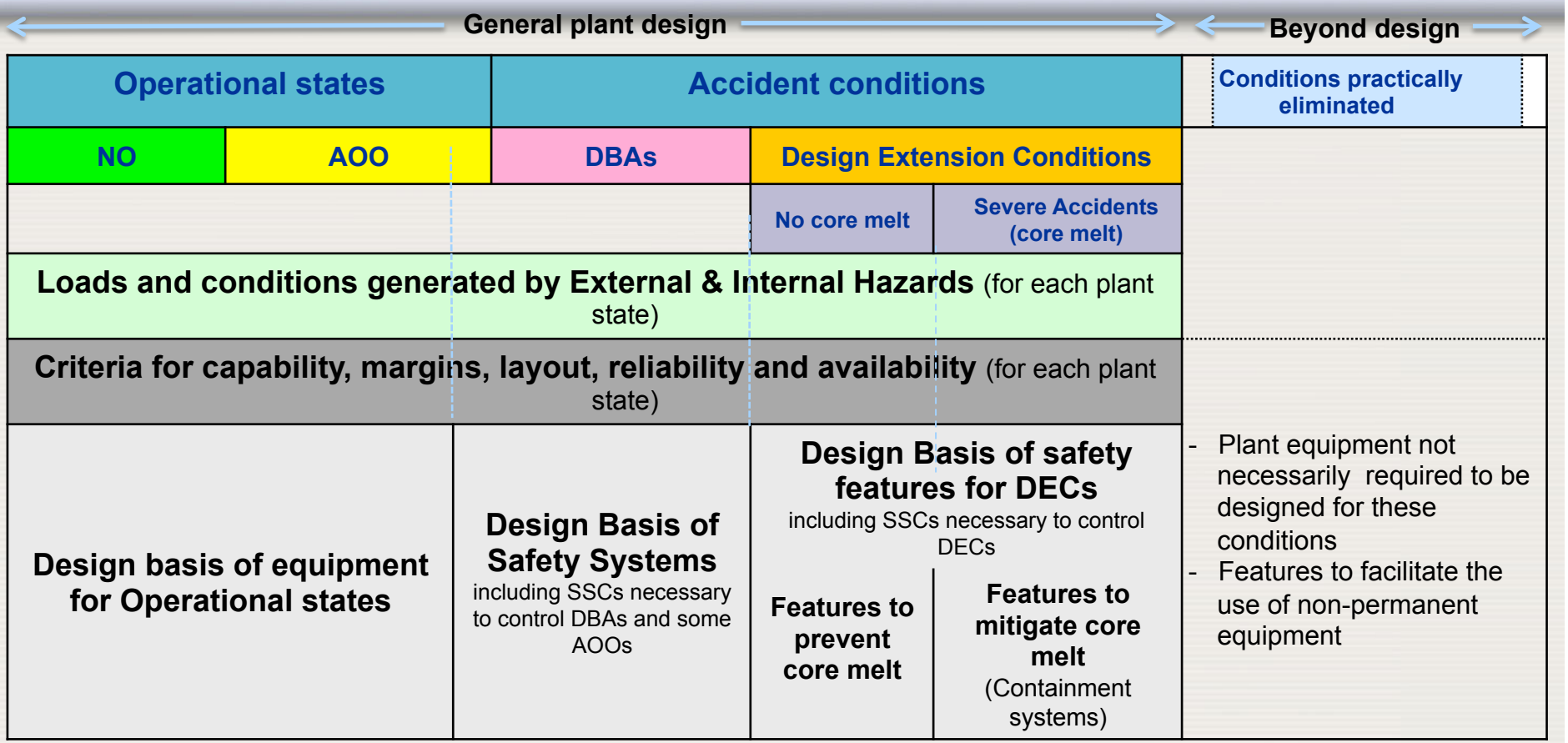
SSR-2/1, 2012

Operational states		Accident conditions			Early or large releases are practically eliminated *
NO	AOO	DBAs	Design Extension Conditions		
			No core melt	Severe Accidents (core melt)	
1st level DiD	2nd level DiD	3rd level DiD	4th level DiD		
Included in the design basis					Beyond design basis

(*) The possibility of certain conditions occurring is considered to have been practically eliminated if it is physically impossible for the conditions to occur or if the conditions can be considered with a high degree of confidence to be extremely unlikely to arise.

IAEA

SSR-2/1 plant states and design basis of plant equipment



The design basis identifies for each structure, system and component (SSC) of the NPP:

- the functions to be performed , the operational states, accident conditions
- the conditions generated by internal and external hazards that the SSC has to withstand
- the acceptance criteria for the necessary capability, reliability, availability and functionality
- specific assumptions and design rules

IAEA

Plant states addressed in the design (1)

Operational states		Accident conditions	
Normal operation	Anticipated operational occurrences	Design Basis Accidents	Design Extension Conditions

Requirement 19: Design basis accidents

A set of accident conditions that are to be considered in the design shall be derived from postulated initiating events for the purpose of establishing the boundary conditions for the plant to withstand without acceptable limits for radiation protection being exceeded.

- DBAs are used to define the design basis of the “safety systems” and for other items important to safety that are necessary to control those accidents (return the plant to a safe state and mitigate the consequences)

- Safety systems are designed with the application of the “single failure criteria”

- Key plant parameters do not exceed specified design limits. No or only minor radiological impacts, both on and off the site, and do not necessitate any off-site intervention measures

- Design Basis Accidents shall be analysed in a conservative manner.

IAEA

Plant states addressed in the design (2)

Operational states		Accident conditions	
Normal operation	Anticipated operational occurrences	Design Basis Accidents	Design Extension Conditions

Requirement 20: Design extension conditions

A set of design extension conditions shall be derived on the basis of engineering judgement, deterministic assessments and probabilistic assessments for the purpose of further improving the safety of the nuclear power plant by enhancing the plant's capabilities to withstand, without unacceptable radiological consequences, accidents that are either more severe than design basis accidents or that involve additional failures. These design extension conditions shall be used to identify the additional accident scenarios to be addressed in the design and to plan practicable provisions for the prevention of such accidents or mitigation of their consequences if they do occur.

-The main purpose of DECs is to ensure that accident conditions not considered as DBAs are prevented and/or mitigated as far as reasonably practicable

- DECs are used to define the design basis for the "safety features" and for the other items important to safety necessary to prevent and to mitigate DECs

- Safety features for DECs are not required to comply with the "single failure criteria"

- Design Extension Conditions can be analysed with a best estimate analysis

Plant states addressed in the design (3)

Operational states		Accident conditions	
Normal operation	Anticipated operational occurrences	Design Basis Accidents	Design Extension Conditions

Qualitative success criteria for Design Extension Conditions

- The integrity of the containment is maintained (the containment shall cope with core melt situation) and the plant can be brought into a controlled state.

- Design provisions shall be such that only protective measures that are of limited scope in terms of area and time are necessary for the protection of the public, and sufficient time is available to implement these measures.

IAEA

Examples of Design Extension Conditions (DECs)

- DECs without core melt
  - anticipated transient without scram (ATWS)
  - station blackout (SBO)
  - loss of core cooling in the residual heat removal mode
  - extended loss of cooling of fuel pool and inventory
  - LOCA plus loss of one emergency core cooling system (either the high pressure or the low pressure emergency cooling system)
  - loss of the component cooling water system or the essential service water system

- DECs with core melt
  - Representative group of severe accident conditions to be used for defining the basis for the design of the mitigative safety features for these conditions.
  - The features for the mitigation of DEC with core melt should be such to prevent that those severe accident phenomena, such as hydrogen detonation, basemat melt through due to core-concrete interaction and steam explosions cause the loss of containment integrity.
  - Maintaining the integrity of the containment is the main objective. This also implies that the cooling and stabilization of the molten fuel and the removal of heat from the containment need to be achieved in the long term.

IAEA Definition of DECs: Postulated accident conditions that are not considered for design basis accidents, but that are considered in the design process of the facility in accordance with best estimate methodology, and for which releases of radioactive material are kept within acceptable limits. Design extension conditions could include severe accident conditions.

Lessons learned from Fukushima (1)

- After the Fukushima event (March 2011) the IAEA has started an action to review and revise, if necessary, all Safety Standards to take into consideration the lessons learned from the accident
- The Safety Standards that needed to be revised have been identified and for each Safety Standard areas that needed improvement or amendment have been identified
- The revision of Safety requirements has been completed and the new publications are in printing
- The revision of Safety Guides is in progress

IAEA

Lessons learned from Fukushima (2)

Amendments to SSR-2/1: Requirements for Design of NPPs

- Defence in depth
  - Further enhancement of the independence of levels 3 and 4
- External events
  - The design of items important to safety shall provide adequate margin to avoid cliff-edge effects
  - The design of items ultimately necessary to prevent early or large releases shall provide adequate margin against natural events exceeding those derived from the site hazard evaluation
- Ultimate heat sink
  - If the availability of the UHS can not be demonstrated for all external hazards, a second diverse UHS shall be provided
- Station blackout
  - An alternate power source shall be available to supply power for DECs
- Use of alternative/mobile equipment
  - The design shall facilitate the use of alternative/mobile equipment 1) for connection of alternative power sources; 2) for cooling the containment for preserving its integrity

IAEA

Glossary (New and revised Definitions)

- **accident conditions**
  Deviations from normal operation less frequent and more severe than anticipated operational occurrences, and which include design basis accidents and design extension conditions.

- **design extension conditions**
  Accident conditions of lower frequency than design basis accidents in which doses or radioactive releases could exceed acceptable limits for design basis accidents. These include conditions with or without significant core degradation.

- s**afety feature for design extension conditions**
  Equipment designed to perform or which has a safety function in design extension conditions.

- **controlled state**
  Plant state, following an anticipated operational occurrence or accident conditions, in which the fundamental safety functions can be ensured and which can be maintained for a time sufficient to implement provisions to reach a safe state.

- **safe state**
  Plant state, following an anticipated operational occurrence or accident conditions, in which the reactor is subcritical and the fundamental safety functions can be ensured and maintained stable for a long time.

- IAEA

...Thank you for your attention

IAEA