IAEA 60 Years
Atoms for Peace and Development

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

ICTP/Trieste, 9 – 20 October 2017

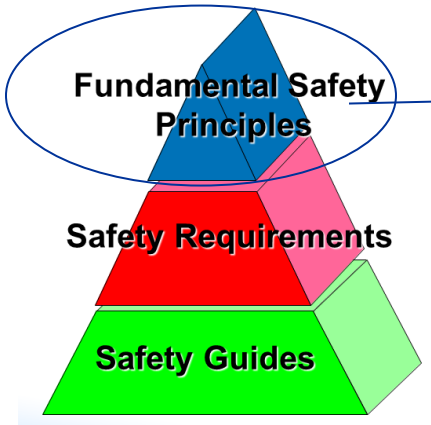
Requirements for NPP Design
Safety Principles and Concepts
Principal Technical Requirements

Javier YLLERA
Safety Assessment Section
Division of Nuclear Installation Safety

Outline

- IAEA Safety Standards for NPP design. An Overview
- Safety Requirements for NPP Design
- Evolution and revision after the Fukushima accident
- Safety Principles and Concepts
- Principal Technical Requirements

IAEA Fundamental Safety Principles (2006)



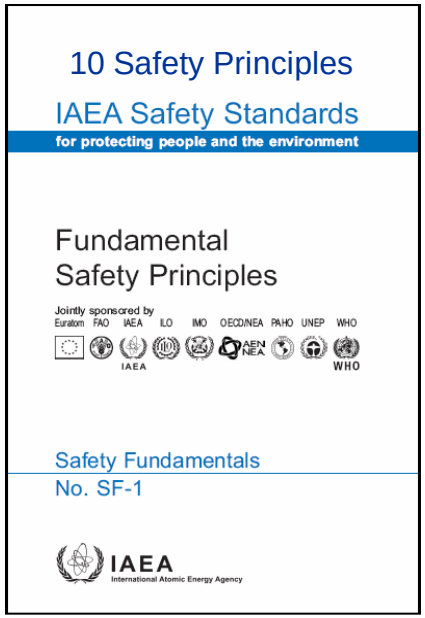
Safety Objective

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

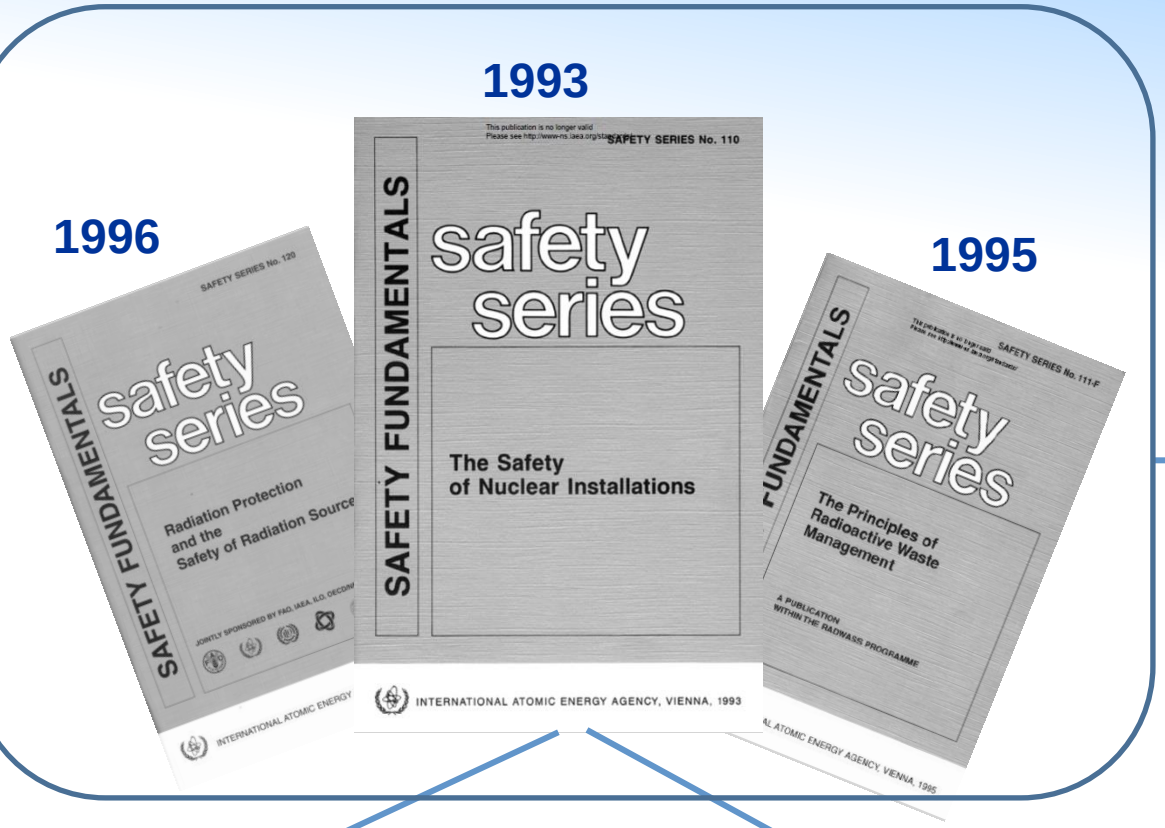
Prevention of Accidents

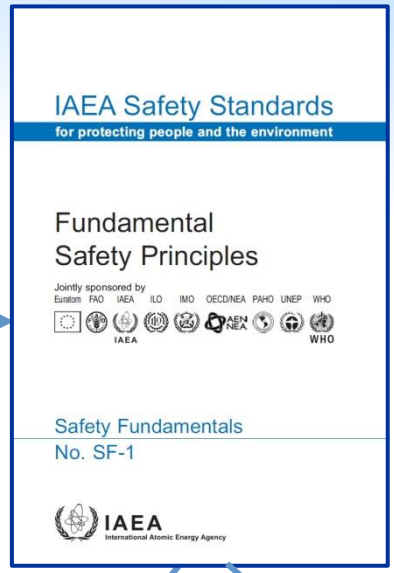
Justification of Facilities and Activities

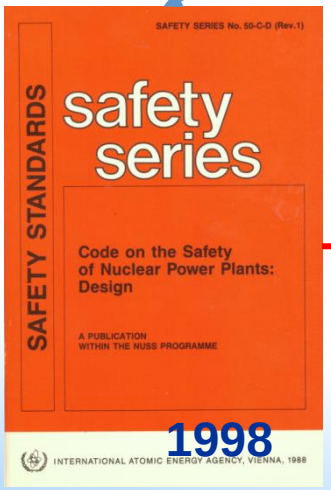
Optimization of Protection

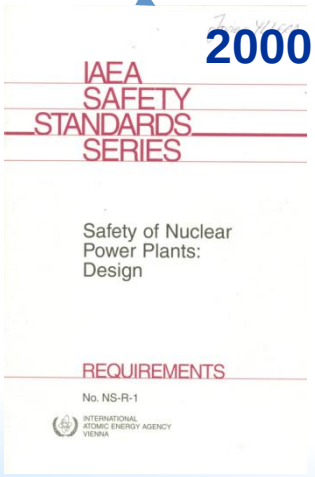
Limitation of Risks to Individuals

Protection of Present and Future Generations


1993
1996
1995
SAFETY SERIES No. 110
SAFETY FUNDAMENTALS
safety series
The Safety of Nuclear Installations
INTERNATIONAL ATOMIC ENERGY AGENCY, VIENNA, 1993
SAFETY SERIES No. 120
Radiation Protection and the Safety of Radiation Source
SAFETY SERIES No. 111-F
The Principles of Radioactive Waste Management
A PUBLICATION WITHIN THE RADWASS PROGRAMME


1996
IAEA Safety Standards
for protecting people and the environment
Fundamental Safety Principles
Jointly sponsored by
Euratom FAO IAEA ILO IMO OECD/NEA PAHO UNEP WHO
Safety Fundamentals
No. SF-1
IAEA
International Atomic Energy Agency

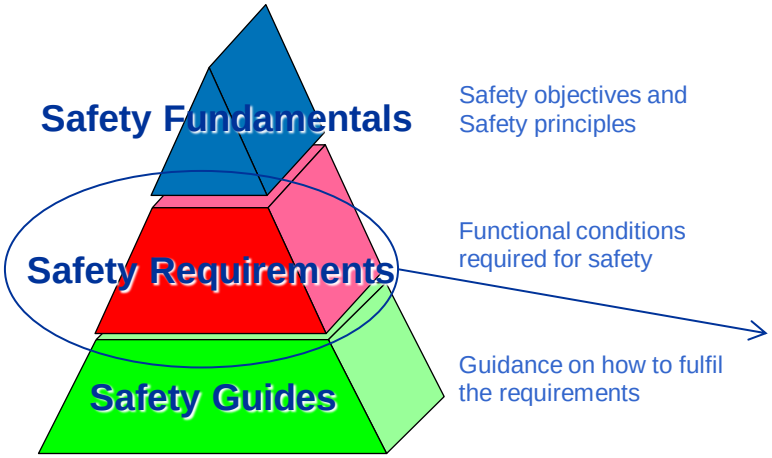

SAFETY SERIES No. 50-C-D (Rev.1)
SAFETY STANDARDS
safety series
Code on the Safety of Nuclear Power Plants: Design
A PUBLICATION WITHIN THE NUSS PROGRAMME
INTERNATIONAL ATOMIC ENERGY AGENCY, VIENNA, 1988
1998


2000
IAEA SAFETY STANDARDS SERIES
Safety of Nuclear Power Plants: Design
REQUIREMENTS
No. NS-R-1
INTERNATIONAL ATOMIC ENERGY AGENCY VIENNA


2012
IAEA Safety Standards
for protecting people and the environment
Safety of Nuclear Power Plants: Design
Specific Safety Requirements
No. SSR-2/1
IAEA
International Atomic Energy Agency


2016
IAEA Safety Standards
for protecting people and the environment
Safety of Nuclear Power Plants: Design
Specific Safety Requirements
No. SSR-2/1 (Rev. 1)
IAEA
International Atomic Energy Agency

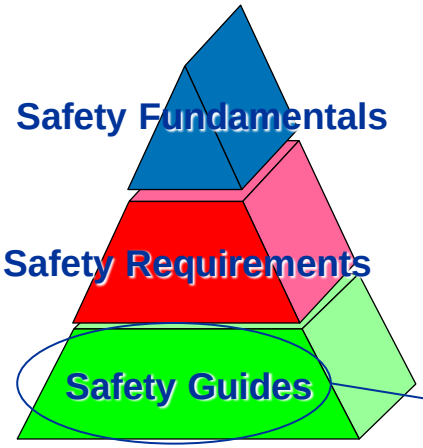
SSR 2/1: Requirements for Design of NPPs



- 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

Issued in 2012
Revised in 2016

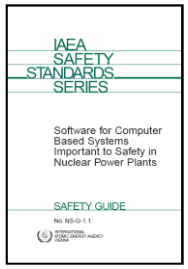
Safety Standards for Design of NPPs

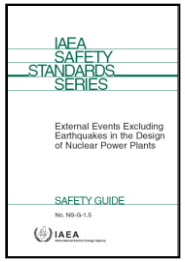


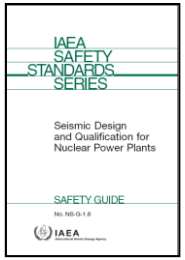
Safety objectives and Safety principles

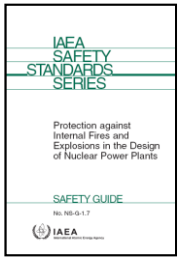
Functional conditions required for safety

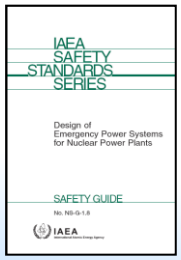
Guidance on how to fulfil the requirements

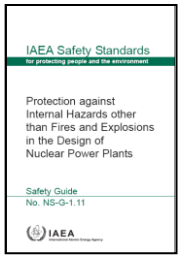


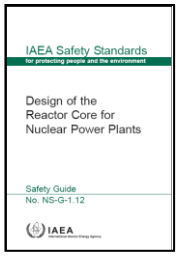


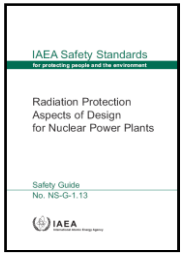


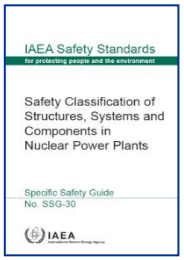












Review and Revision of the Safety Guides

- Current status of revision of safety guides most relevant to NPPs:
  - GS-G-4.1 Format and Content of the Safety Analysis report for Nuclear Power Plants (2004). Draft submission to NUSSC in 2016
  - SSG-30 Safety Classification of Structures, Systems and Components in Nuclear Power Plants (2014)
  - SSG-39: Design of I & C Systems for NPPs (2016)
  - NS-G-1.4 Design of Fuel Handling and Storage Systems for Nuclear Power Plants (2003). Revised draft in preparation. Submission to NUSSC in 2016
  - NS-G-1.6 Seismic Design and Qualification for Nuclear Power Plants (2003). Draft in preparation.
  - NS-G-1.7 Protection against Internal Fires and Explosions in the Design of Nuclear Power Plants (2004) and NS-G-1.11 Protection against Internal Hazards other than Fires and Explosions in the Design of Nuclear Power Plants (2004). Draft for a revised safety guide combining both in preparation.
  - SSG-34 Design of Electrical Power Systems for Nuclear Power Plants (2016)

Review and Revision of the Safety Guides

- Current status of revision of safety guides most relevant to NPPs:

  - NS-G-1.9 Design of the Reactor Coolant System and Associated Systems in Nuclear Power Plants (2004). Draft submitted to NUSSC
  - NS-G-1.10 Design of Reactor Containment Systems for Nuclear Power Plants (2004). Draft in preparation. Submission to MSs in 2017
  - NS-G-1.12 Design of the Reactor Core for Nuclear Power Plants (2005). Draft in preparation. Submission to MSs in 2017
  - NS-G-2.15 Severe Accident Management Programmes for Nuclear Power Plants (2009). MSs comments addressed. Submission to CSS after review by technical editors in 2017
  - SSG-2 Deterministic Safety Analysis for Nuclear Power Plants (2009). Draft in preparation. Submission to MSs in 2017

More information on Status of Safety Guides under:

http://www-ns.iaea.org/standards/

SSR 2/1 - Applicability

- Primarily for land based stationary nuclear power plants with water cooled reactors
- It may be used, with judgement, for application to other reactor types, to determine the requirements that have to be considered in developing the design.

- It might not be practicable to apply all the requirements to nuclear power plants that are already in operation.
- It is expected that a comparison will be made against the current standards, for example as part of the periodic safety review for the plant

Importance of the Requirements for the Design of NPPs

- Define the 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
  - document of large consensus

- Provide the links with the requirements for site evaluation and for operation
  - taking into consideration the impact of the site on the design
  - ensuring the safe operation and maintenance of the plant

Importance of the Requirements for the Design of NPPs

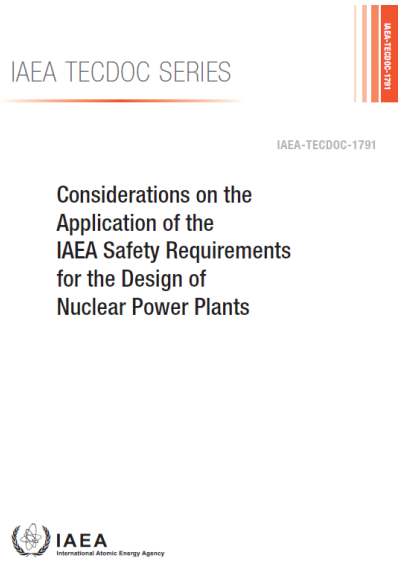
- are the main reference to perform design safety reviews
- significantly contributed to establishing a common safety approach and terminology
- used as reference for establishing licensing regulations in several countries
  - adopted as national regulation
  - used to integrate existing national regulations

Revision of SSR 2/1 after the Fukushima Daiichi accident

Overview of Main Changes

- Reinforcement of DiD and the independence of DiD provisions, in particular those for severe accidents
- Stressing the need for margins to avoid cliff edge effects. More margins for items that ultimately prevent large or early releases
- Interconnection of units without sharing safety systems /DEC features
- Reinforced capabilities for heat transfer to the UHS.
- Implementation of features (design, procedures, etc.) to enable the use (e.g. hook-up) of non permanent equipment
- Reinforced capabilities for power supply in DECs.
- Additional measures for spent fuel pool instrumentation, cooling and maintaining inventory.

TECDOC 1791:
Considerations on the Application of the IAEA Safety Requirements for the Design of Nuclear Power Plants



- Aimed at facilitating the understanding and providing more explicit information on selected new topics and terms introduced in the requirements for which there is not always a common understanding in different Member States.

Structure of SSR 2/1

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

- **Section 3 :** Requirements on Management of Safety in design

- **Sections 4:** Principal Technical Requirements

- **Sections 5:** General Plant Design

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

  Reactor core, Reactor coolant systems, Containment systems, I&C, Emergency power supply, fuel handling and storage systems, etc.

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

- INTRODUCTION
- APPLYING SAFETY PRINCIPLES AND CONCEPTS
- MANAGEMENT OF SAFETY IN DESIGN
  - 3 Requirements
- PRINCIPAL TECHNICAL REQUIREMENTS
  - Fundamental safety functions, Radiation protection in design, Design for a nuclear power plant , Application of defence in depth, Interfaces of safety with security and safeguards, Proven engineering practices, Safety assessment, Provision for construction, Features to facilitate radioactive waste management and decommissioning
- 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)

Safety objectives; Radiation protection; Defence in depth

82 Overarching Requirements

Safety Principles and Concepts

Applying the Safety Principles and Concepts

- The Fundamental Safety Principles (FSPs) establish **one fundamental safety objective** (FSO) and **ten safety principles** that provide the basis for requirements and measures for the protection of people and the environment against radiation risks.
- Measures have to be taken to achieve the following:
  - To control the radiation exposure of people and radioactive releases to the environment in operational states;
  - To restrict the likelihood of events that might lead to a loss of control over a the nuclear reactor core or any other source of radiation at a nuclear power plant;
  - To mitigate the consequences of such events if they were to occur.
- It applies for all stages in lifetime of an NPP

Safety Principle 8: Prevention of Accidents

All practical efforts must be made

to prevent and mitigate nuclear or radiation accidents

- **The primary means of preventing and mitigating the consequences of accidents is "defence in depth"**
  - Defence in depth is implemented primarily through the combination of a number of **consecutive and independent levels of protection**
  - When properly implemented, defence in depth ensures that no single technical, human or organizational failure could lead to harmful effects, and that the combinations of failures that could give rise to significant harmful effects are of very low probability.
  - The **independent effectiveness** of the different levels of defence is a necessary element of defence in depth.

Safety Principle 8: Prevention of Accidents

IAEA 60 Years Atoms for Peace and Development

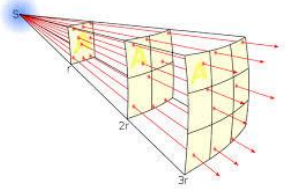
Defence in depth is provided by an appropriate combination of:

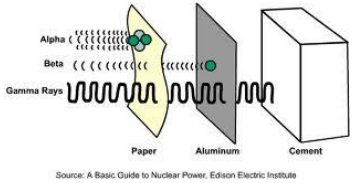
- An effective management system, strong commitment to safety and strong safety culture
- Adequate site selection and the incorporation of good design and engineering features providing safety margins, diversity and redundancy mainly by the use of:
  - Design, technology and materials of high quality and reliability
  - Control, limiting and protection systems and surveillance features
  - Appropriate combination of inherent and engineered safety features
- Comprehensive operational and accident management procedures and practices

Defence in Depth (DiD)

- **DiD is implemented through the combination of a number of consecutive and independent levels of protection.**

- **<u>Primary physical means of protection</u>:**
  - Barriers for: Confinement and/or Shielding
  - Distance: $\Phi = L / (4 \pi \mathbf{r^2})$

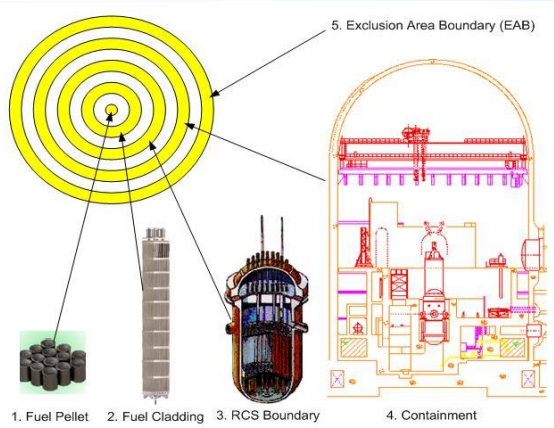




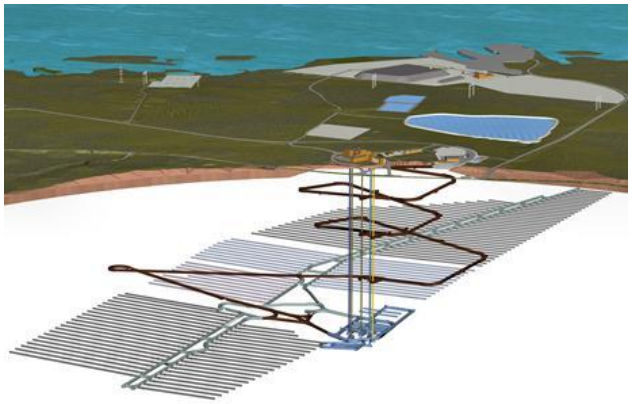
- Implementation of DiD requires barriers. However a barrier should not be confused with a level of defence in depth (often misinterpretation).

- The integrity of the barriers may be challenged by external agents as well as by the internal energy (<u>nuclear reactions</u>, pressure/temperature, etc.). It is necessary to ensure adequate protection of the barriers

Different barriers are needed depending on the radiation source



Physical barriers between reactor core and the environment



Foundations of NPP Safety

Fundamental Safety Principles

Safety Objective:

Protect people and the environment from effects of radiation

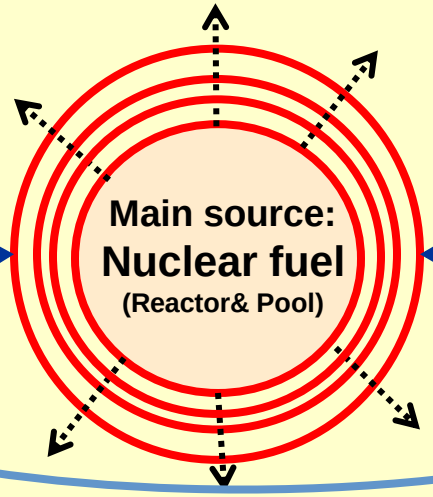
- **10 Safety principles:**

No. 8: Prevention and mitigation of accidents

Defence in depth

Based on a number of consecutive levels of protection

including physical barriers.



Fundamental Safety Functions

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

The current implementation of DiD at nuclear power plants comprises **5 levels** of protection and it is based on 4 physical barriers (fuel matrix, fuel cladding, reactor coolant boundary and containment building)

Radiation Protection in Design

- It is required to ensure that **for all operational states** of a nuclear power plant and for any associated activities, **doses** from exposure to radiation within the installation or exposure due to any planned radioactive release from the installation **are kept below the dose limits** and kept **as low as reasonably achievable**. In addition, it is required to take **measures for mitigating the radiological consequences of any accidents**, if they were to occur.
- It is also required that nuclear power plants be designed and operated so as to **keep all sources of radiation under strict technical and administrative control**. However, this principle does not preclude limited exposures or the release of authorized amounts of radioactive substances to the environment from nuclear power plants in operational states. Such exposures and radioactive releases are required to be strictly controlled and to be kept **as low as reasonably achievable**, in compliance with regulatory and operational limits as well as radiation protection requirements.

Safety in Design (1/3)

To achieve the highest level of safety that can reasonably be achieved in the design of a nuclear power plant, **measures are required** to be taken to do the following, consistent with national acceptance criteria and safety objectives:

- **To prevent accidents** with harmful consequences resulting from a loss of control over the reactor core or over other sources of radiation, and to mitigate the consequences of any accidents that do occur;
- To ensure that **for all accidents taken into account in the design** of the installation, any **radiological consequences would be below the relevant limits** and would be kept as low as reasonably achievable;
- To ensure that the **likelihood of occurrence of an accident with serious radiological consequences is extremely low** and that the radiological consequences of such an accident would be mitigated to the fullest extent practicable.

Safety in Design (2/3)

- To demonstrate that the FSO is achieved in the design of a nuclear power plant, a **comprehensive safety assessment** of the design is required to be carried out. Its objective is to identify all possible sources of radiation and to evaluate possible doses that could be received by workers at the installation and by members of the public, as well as possible effects on the environment, as a result of operation of the plant.

- The safety assessment is required in order to examine:
  - (i) normal operation of the plant;
  - (ii) the performance of the plant in anticipated operational occurrences; and
  - (iii) accident conditions.

- On the basis of this analysis, the capability of the design to withstand postulated initiating events and accidents can be established, the effectiveness of the items important to safety can be demonstrated and the inputs (prerequisites) for emergency planning can be established.

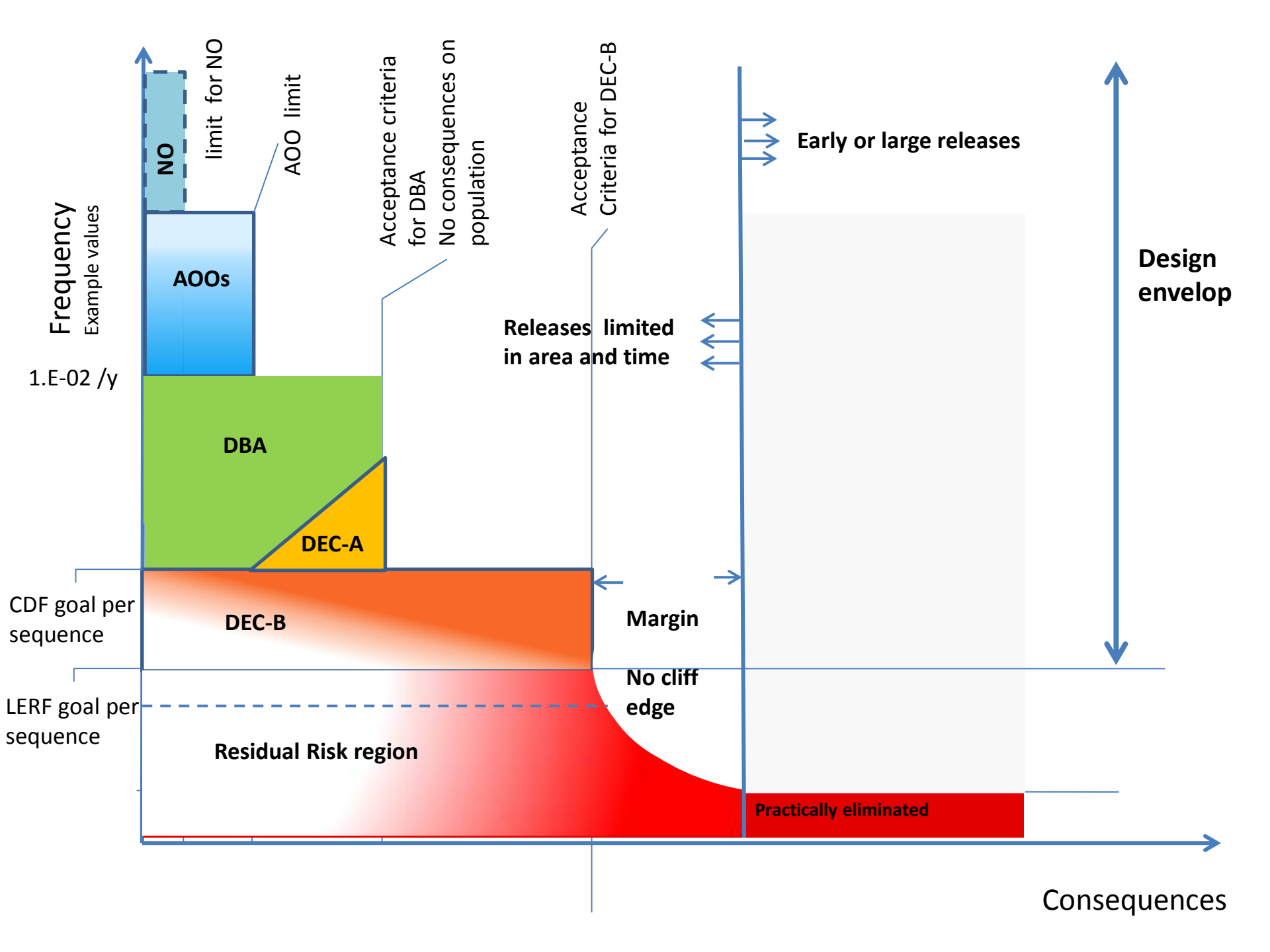
Safety in Design (3/3)

- Measures are required to be taken to control exposure for all operational states at levels that are ALARA and to **minimize the likelihood of an accident** that could lead to the loss of control over a source of radiation.

- Measures are required to be taken to ensure that the **radiological consequences of an accident would be mitigated**. Such measures include the provision of **safety features and safety systems**, the establishment of **accident management procedures** by the operating organization and, possibly, the establishment of off-site protective actions.

- The design for safety of a nuclear power plant applies the safety principle that practical measures must be taken to mitigate the consequences for human life and health and for the environment of nuclear or radiation accidents

- Plant event sequences that could result in high radiation doses or in a large radioactive release have to be **'practically eliminated'** and plant event sequences with a significant frequency of occurrence have to have no, or only minor, potential radiological consequences. An essential objective is that the **necessity for off-site protective actions to mitigate radiological consequences be limited or even eliminated in technical terms**.


Frequency
Example values
1.E-02 /y
NO
limit for NO
AOO limit
AOOs
Acceptance criteria for DBA
No consequences on population
DBA
DEC-A
Acceptance Criteria for DEC-B
Releases limited in area and time
Early or large releases
Design envelop
CDF goal per sequence
DEC-B
Margin
No cliff edge
LERF goal per sequence
Residual Risk region
Practically eliminated
Consequences

DiD: 1st Level. Definition in SSR 2/1

- **The purpose of the first level of defence is to prevent deviations from normal operation and the failure of items important to safety**.

- This leads to requirements that the plant be soundly and conservatively sited, designed, constructed, maintained and operated in accordance with quality management and appropriate and proven engineering practices.

- To meet these objectives, careful attention is paid to the selection of appropriate design codes and materials, and to the quality control of the manufacture of components and construction of the plant, as well as to its commissioning.

DiD: 1st Level. Definition in SSR 2/1 (cont.)

- Design options that reduce the potential for internal hazards contribute to the prevention of accidents at this level of defence.

- Attention is also paid to the processes and procedures involved in design, manufacture, construction and in-service inspection, maintenance and testing, to the ease of access for these activities, and to the way the plant is operated and to how operating experience is utilized.

- This process is supported by a detailed analysis that determines the requirements for operation and maintenance of the plant and the requirements for quality management for operational and maintenance practices.

DiD: 2nd Level. Definition in SSR 2/1

- **The purpose of the second level of defence is to detect and control deviations from normal operational states in order to prevent anticipated operational occurrences at the plant from escalating to accident conditions**.
- This is in recognition of the fact that postulated initiating events are likely to occur over the operating lifetime of a nuclear power plant, despite the care taken to prevent them.
- This second level of defence necessitates the provision of specific systems and features in the design, the confirmation of their effectiveness through safety analysis, and the establishment of operating procedures to prevent such initiating events, or else to minimize their consequences, and to return the plant to a safe state.

DiD: 3rd Level. Definition in SSR 2/1

- For the third level of defence, it is assumed that, although very unlikely, the escalation of certain anticipated operational occurrences or postulated initiating events might not be controlled at a preceding level and that an accident could develop.

- In the design of the plant, such accidents are postulated to occur.

- **This leads to the requirement that inherent and/or engineered safety features, safety systems and procedures be provided that are capable of preventing damage to the reactor core** or significant off-site releases and returning the plant to a safe state.

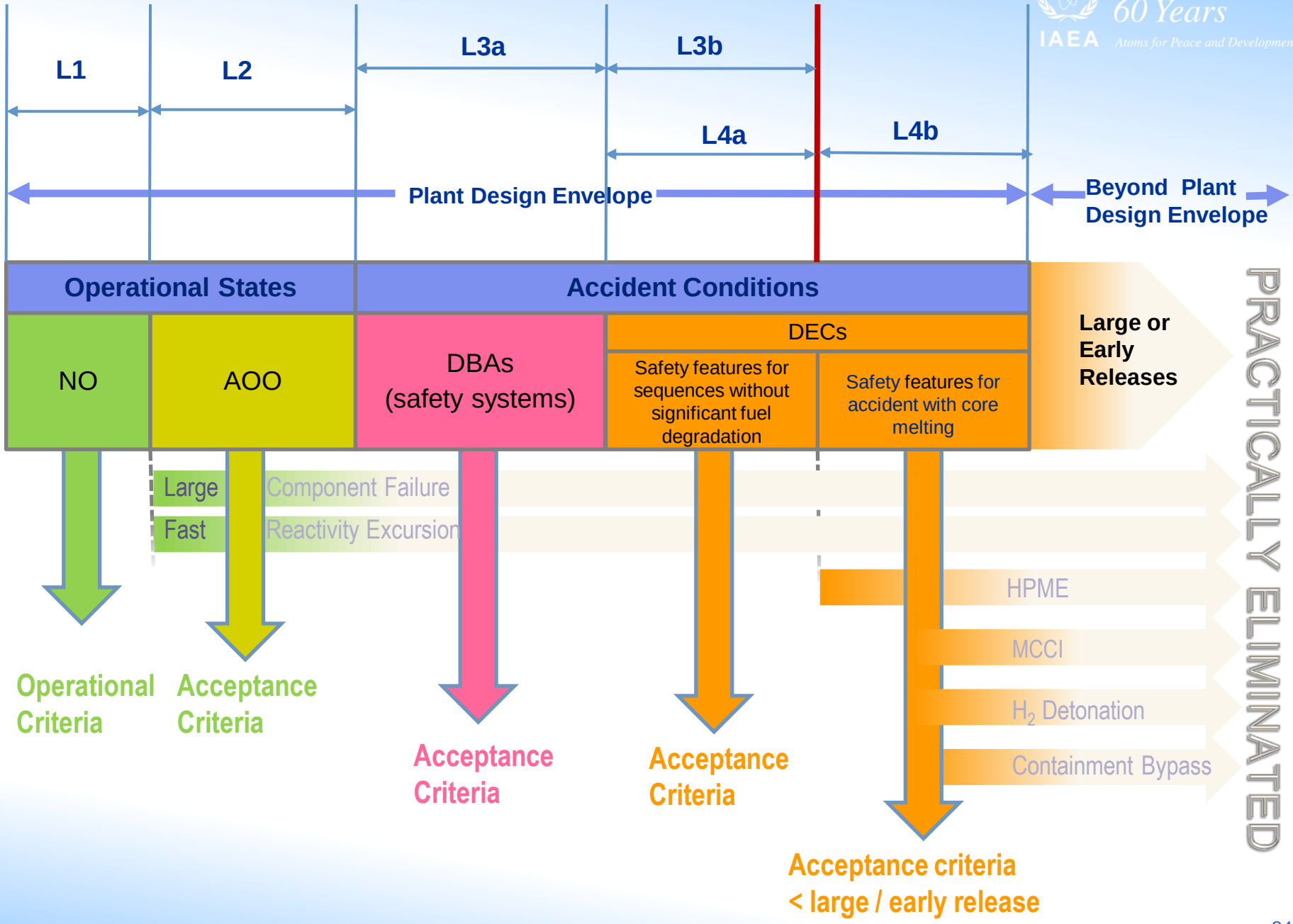
DiD: 4th Level. Definition in SSR 2/1

- **The purpose of the fourth level of defence is to mitigate the consequences of accidents that result from failure of the third level of defence in depth**.
- This is achieved by preventing the progression of the accident and mitigating the consequences of a severe accident.
- The safety objective in the case of a severe accident is that only protective measures that are limited in terms of times and areas of application would be necessary and that off-site contamination would be avoided.
- Sequences that lead to large or early radioactive releases are required to be ‘practically eliminated’.

DiD: 5th Level. Definition in SSR 2/1

- The purpose of the fifth and final level of defence is to mitigate the radiological consequences of radioactive releases that could potentially result from accidents.

- This requires the provision of an adequately equipped emergency control centre and emergency plans and emergency procedures for on-site and off-site emergency response.


L1
L2
L3a
L3b
L4a
L4b
Plant Design Envelope
Beyond Plant Design Envelope
Operational States
Accident Conditions
NO
AOO
DBAs (safety systems)
DECs
Safety features for sequences without significant fuel degradation
Safety features for accident with core melting
Large or Early Releases
Large
Component Failure
Fast
Reactivity Excursion
HPME
MCCI
H_2 Detonation
Containment Bypass
PRACTICALLY ELIMINATED
Operational Criteria
Acceptance Criteria
Acceptance Criteria
Acceptance Criteria
Acceptance criteria < large / early release

Tablefrom Tecdoc 1791 on application of safety requirements

Level of defence	Objective	Associated plant state	Criteria for maintaining integrity of barriers	Criteria for limitation of radiological consequences
Level 1	Prevention of abnormal operation and failures	Normal operation	No failure of any of the physical barriers except minor operational leakages	Negligible radiological impact beyond immediate vicinity of the plant. Acceptable effective dose limits are bounded by the general radiation protection limit for the public (1 mSv /year commensurate with typical doses due to natural background), typically in the order of 0.1 mSv/year.
Level 2	Control of abnormal operation and detection of failures	Anticipated operational occurrence	No failure of any of the physical barriers except minor operational leakages	Negligible radiological impact beyond immediate vicinity of the plant. Acceptable effective dose limits are similar as for normal operation, limiting the impact per event and for the period of 1 year following the event (0.1 mSv/y)
Level 3a	Control of design basis accidents (DBAs)	Design basis accident	No consequential damage of the reactor coolant system, maintaining containment integrity, limited damage of the fuel	No or only minor radiological impact beyond immediate vicinity of the plant, without the need for any off-site emergency actions. Acceptable effective dose limits are typically in the order of few mSv.
Level 3b	Control of DECs without significant fuel degradation (prevention of accident progression into severe accident)	Design extension conditions without significant fuel degradation	No consequential damage of the reactor coolant system, maintaining containment integrity, limited damage of the fuel.	The same or similar radiological acceptance criteria as for the most unlikely design basis accidents
Level 4	Control of DECs with core melt (mitigation of consequences of severe accidents)	Design extension conditions with core melt (severe accident)	Maintaining containment integrity	Only emergency countermeasures that are of limited scope in terms of area and time are necessary
Level 5	Mitigation of radiological consequences of significant releases	Accidents with releases requiring implementation of emergency countermeasures	Containment integrity severely impacted, or containment disabled or bypassed	Off site radiological impact necessitating emergency countermeasures

- **Sections 1-2 :** Introduction, Principles and Concepts
- **Section 3 :** Requirements on Management of Safety in design **REQUIREMENTS 1 TO 3**
- **Sections 4:** Principal Technical Requirements
- **Sections 5:** General Plant Design
- **Section 6:** Requirements for specific plant systems:

  Reactor core, Reactor coolant systems, Containment systems, I&C, Emergency power supply, fuel handling and storage systems, etc.

Management of Safety in Design

- **Requirement 1: Responsibilities in the management of safety in plant design**

An applicant for a license to construct and/or operate a nuclear power plant shall be responsible for ensuring that the design submitted to the regulatory body meets all applicable safety requirements.

– All organizations, including the design organization, engaged in activities important to the safety of the design of a nuclear power plant shall be responsible for ensuring that safety matters are given the highest priority.

The design organization is the organization responsible for preparation of the final detailed design of the plant to be built

Management of Safety in Design

- **Requirement 2: Management system for plant design**

  The design organization shall establish and implement a management system for ensuring that all safety requirements established for the design of the plant are considered and implemented in all phases of the design process and that they are met in the final design.

- **Requirement 3: Safety of the plant design throughout the lifetime of the plant**

  The operating organization shall establish a formal system for ensuring the continuing safety of the plant design throughout the lifetime of the nuclear power plant.

- **Sections 1-2 :** Introduction, Principles and Concepts
- **Section 3 :** Requirements on Management of Safety in design
- **Sections 4: Principal Technical Requirements**
  REQUIREMENTS 4 TO 12
- **Sections 5:** General Plant Design
- **Section 6:** Requirements for specific plant systems:

  Reactor core, Reactor coolant systems, Containment systems, I&C, Emergency power supply, fuel handling and storage systems, etc.

Principal Technical Requirements

- **Requirement 4: Fundamental safety functions (FSFs)**

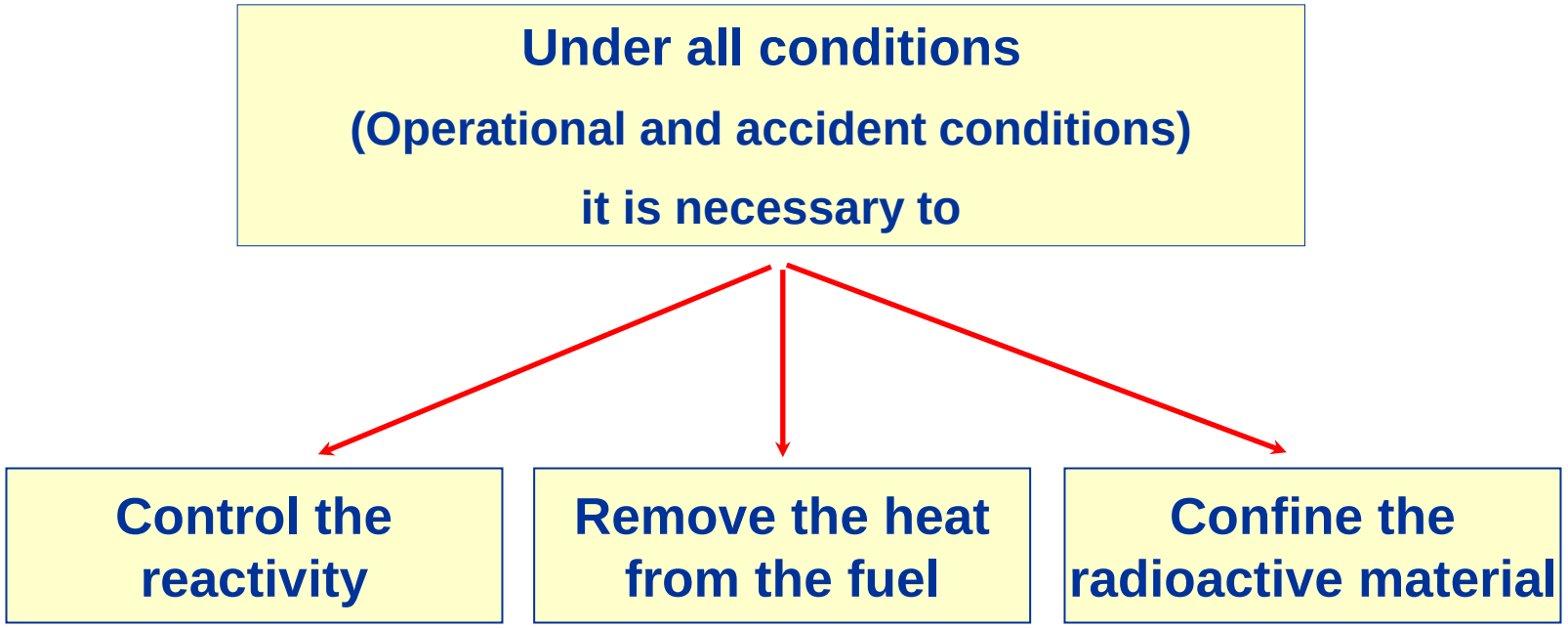
  Fulfilment of the following fundamental safety functions for a nuclear power plant shall be ensured for all plant states

  – Control of reactivity
  – Removing heat from the fuel
  – Confinement of radioactive materials, shielding against radiation and control of operational discharges as well as limitation of accidental releases

  – A systematic approach shall be taken to identifying those items important to safety that are necessary to fulfil the FSFs functions and to identifying the inherent features that are contributing to fulfilling, or that are affecting, the fundamental safety functions for all plant states.

  – Means of monitoring the status of the plant shall be provided for ensuring that the required safety functions are fulfilled.

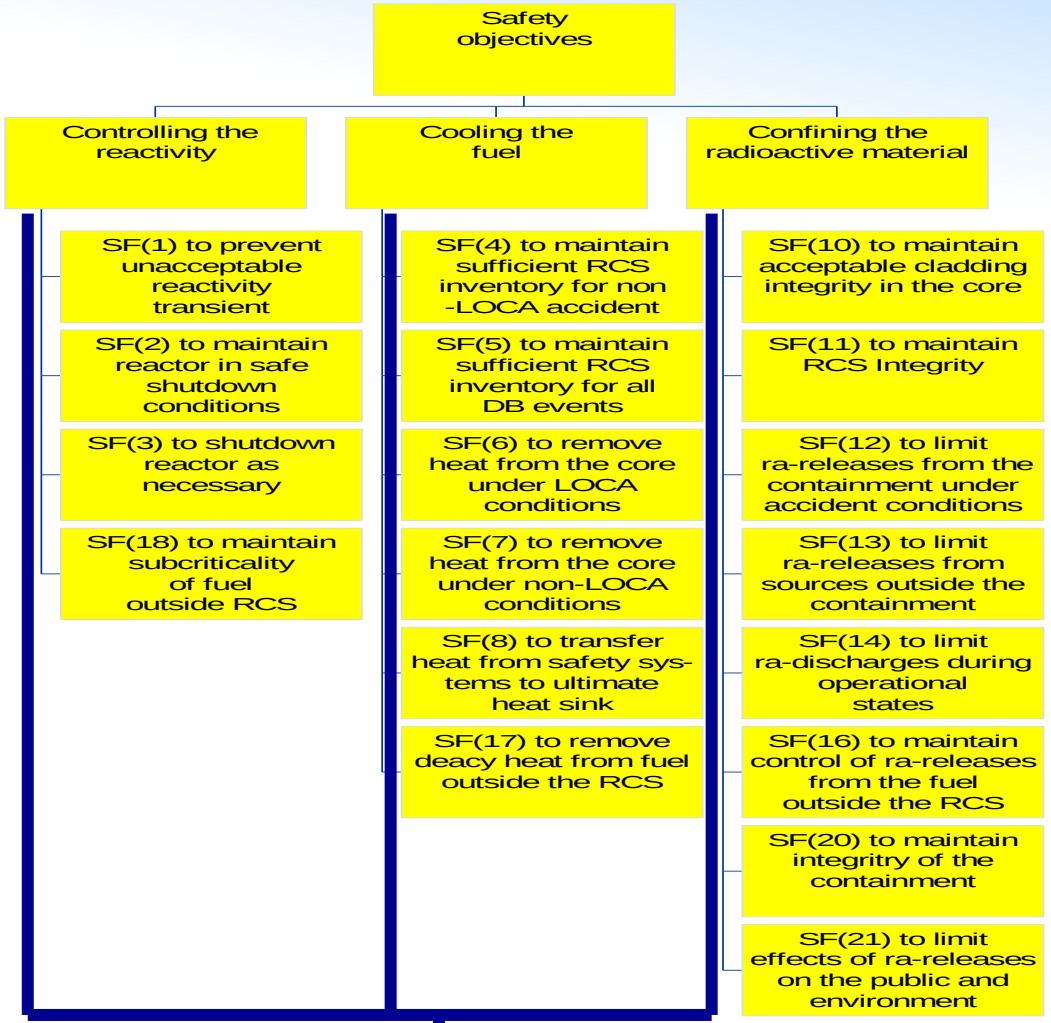
Three Fundamental Safety Functions



Fundamental and subordinated safety functions. Examples

Fundamental safety functions

Subordinated safety functions applicable for LWRs



Principal Technical Requirements

- **Requirement 5: Radiation protection**

  The design of a nuclear power plant shall be such as to ensure that radiation doses to workers at the plant and to members of the public:

  - **do not exceed authorized limits and are kept as low as reasonably achievable in normal operation and anticipated operational occurrences and during decommissioning, and**
  - **remain below acceptable limits during and following accident conditions.**

  - The design shall be such as to ensure that plant states that could lead to high radiation doses or large radioactive releases are practically eliminated and that there are no, or only minor, potential radiological consequences for plant states with a significant likelihood of occurrence.
  - Acceptable limits for radiation protection associated with the relevant categories of plant states shall be established, consistent with the regulatory requirements.

Principal Technical Requirements

- **Requirement 6: Design for a nuclear power plant**

  The design for a nuclear power plant shall ensure that the plant and items important to safety have the appropriate characteristics to ensure that safety functions can be performed with the necessary reliability, that the plant can be operated safely within the operational limits and conditions for the full duration of its design life and can be safely decommissioned, and that impacts on the environment are minimized.

  – The design shall meet the requirements of the owner and the operating organization, the requirements of the regulatory body and the requirements of relevant legislation, and relevant and applicable national and international codes and standards

  – due account is taken of human capabilities and limitations and factors that could influence human performance

  – due account of relevant available experience that has been gained in the design, construction and operation of other plants and of the results of relevant research programmes.

  – due account of the results of deterministic and probabilistic safety analyses, and an iterative process shall be carried out by means of which it shall be ensured that due consideration has been given to the prevention of accidents and the mitigation of their consequences.

  – the generation of radioactive waste and radioactive discharges are kept as low as reasonably achievable

Principal Technical Requirements

- **Requirement 7: Application of defence in depth**

  The design of a nuclear power plant shall incorporate defence in depth. The levels of defence in depth shall be independent as far as is practicable.

  – The existence of multiple levels of defence is not a basis for continued operation in the absence of one level of defence. All levels of defence in depth shall be kept available at all times.

  – Relaxations shall be justified for specific modes of operation

Principal Technical Requirements

- **Requirement 7: Application of defence in depth**

  …

  – **The design**:
    - Shall provide for multiple physical barriers to the release of radioactive material;
    - Shall be conservative, and the construction shall be of high quality, so as to minimize failures, prevent accidents as far as is practicable and avoid cliff edge effects;
    - Shall provide for the control of plant behaviour by means of inherent and engineered features, such that failures and deviations from normal operation requiring actuation of safety systems are minimized or excluded by design, to the extent possible;
    - Shall provide for supplementing the control of the plant by means of automatic actuation of safety systems, such that failures can be controlled with a high level of confidence, and the need for operator actions in an early phase is minimized;
    - Shall provide for SSCs and procedures to control the course of and, as far as practicable, to limit the consequences of failures and deviations from normal operation that exceed the capability of safety systems;
    - Shall provide multiple means for ensuring that each of the fundamental safety functions is performed, thereby ensuring the effectiveness of the barriers

Principal Technical Requirements

- **Requirement 7: Application of defence in depth (cont.)**

  …

  – The design shall be such as to ensure, as far as is practicable, that the first, or at most the second, level of defence is capable of preventing an escalation to accident conditions for all failures or deviations from normal operation that are likely to occur over the operating lifetime of the nuclear power plant.

  – The levels of defence in depth shall be independent as far as practicable to avoid a failure of one level reducing the effectiveness of other levels. In particular, safety features for design extension conditions (especially features for mitigating the consequences of accidents involving the melting of fuel) shall be as far as is practicable independent of safety systems.

Principal Technical Requirements

- **Requirement 8: Interfaces of safety with security and safeguards**

  Safety measures, nuclear security measures and arrangements for the State system of accounting for, and control of, nuclear material for a nuclear power plant shall be designed and implemented in an integrated manner so that they do not compromise one another.

- **Requirement 9: Proven engineering practices**

  Items important to safety for a nuclear power plant shall be designed in accordance with the relevant national and international codes and standards.

Principal Technical Requirements

- **Requirement 10: Safety assessment**

  Comprehensive deterministic safety assessments and probabilistic safety assessments shall be carried out throughout the design process to ensure that all relevant safety requirements are met by the design of the plant throughout all stages of the plant's lifetime, and to confirm that the design meets requirements as delivered for fabrication, for construction, as built, as operated and as modified.

- **Requirement 11: Provision for construction**

  Items important to safety shall be designed to be manufactured, constructed, assembled, installed and erected in accordance with established processes that ensure the achievement of the design specifications and the required safety performance.

Principal Technical Requirements

- **Requirement 12: Features to facilitate radioactive waste management and decommissioning**

Special consideration shall be given at the design stage of a nuclear power plant to the incorporation of features to facilitate radioactive waste management and the future decommissioning and dismantling of the plant.

- **Sections 1-2 :** Introduction, Principles and Concepts
- **Section 3 :** Requirements on Management of Safety in design
- **Sections 4:** Principal Technical Requirements
- **Sections 5:** General Plant Design. **REQUIREMENTS 13-42**
- **Section 6:** Requirements for specific plant systems e.g.:

  Reactor core, Reactor coolant systems, Containment systems, I&C, Emergency power supply, fuel handling and storage systems

General Plant Design

- Design Basis
  - Plant States
  - Design basis of items important to safety
  - Postulated Initiating events
  - Internal and external hazards
  - Design rules
  - Design extension conditions
  - Safety classification
  - Single failure criterion
  - Common cause failures
- Design for safe operation over the lifetime of the plant
- Human Factors
- Safety Analysis

Design Basis

- **Requirement 13: Categories of plant states**

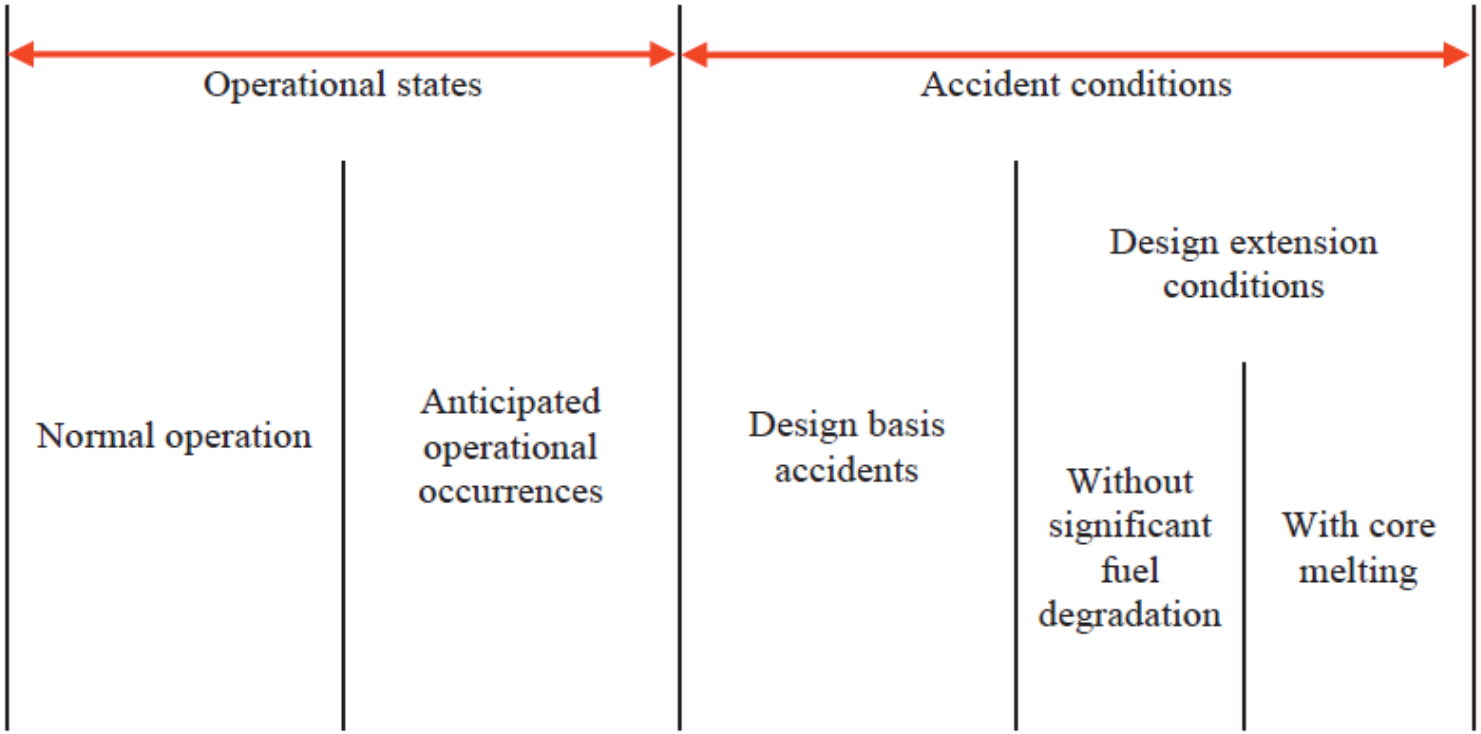
  Plant states shall be identified and shall be grouped into a limited number of categories according to their frequency of occurrence, typically:

  - Normal operation;
  - Anticipated operational occurrences, which are expected to occur over the operating lifetime of the plant;
  - Design basis accidents;
  - Design extension conditions, including accidents with core melting.

  Criteria shall be assigned to each plant state, such that frequently occurring plant states shall have no, or only minor, radiological consequences and plant states that could give rise to serious consequences shall have a very low frequency of occurrence.

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

plant states *(considered in design)*



accident conditions. Deviations from normal operation that are less frequent and more severe than anticipated operational occurrences.

ⓘ Accident conditions comprise design basis accidents and design extension conditions.

Design Basis

- **Requirement 14: Design basis for items important to safety**

  The design of items important to safety shall specify the necessary capability, reliability and functionality for the required plant operational states, for accident conditions and conditions generated by internal and external hazards, to meet the specified acceptance criteria for the lifetime of the plant.

  The design basis for each item important to safety shall be systematically justified and documented

- **Requirement 15: Design limits**

  A set of design limits consistent with the key physical parameters for each item important to safety shall be specified for all operational states and accident conditions.

  Design limits shall be consistent with regulations and standards

Design Basis

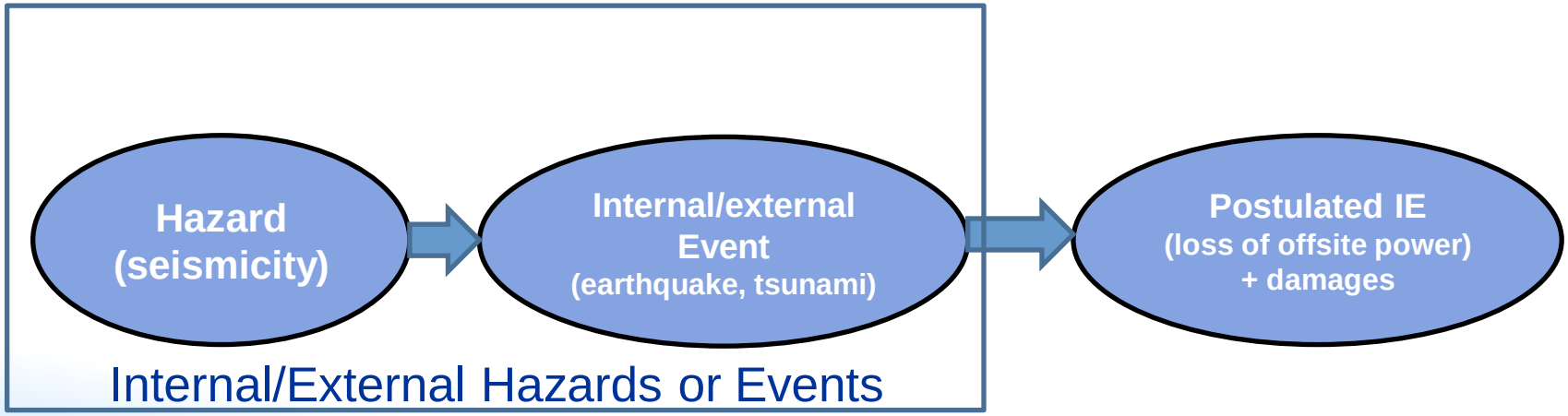
- **Requirement 16: Postulated initiating events**

The design shall apply a systematic approach to identifying a comprehensive set of postulated initiating events such that all credible events with the potential for serious consequences and all credible events with a significant frequency of occurrence have been anticipated and have been considered in the design.

– The postulated initiating events shall be identified on the basis of engineering judgement and a combination of deterministic assessment and probabilistic assessment.
– The postulated initiating events shall include all foreseeable failures of structures, systems and components of the plant, as well as operating errors and possible failures arising from internal and external hazards
– The expected plant response to any postulated initiating event shall be such that the following can reasonably be achieved, in order of preference by : inherent plant characteristics, passive safety features or by the action of systems in operation, safety systems, specified procedural actions.

Internal and External Hazards

- The hazard describes the circumstances that may lead to an event, e.g. the presence of combustible material may lead to a fire. However, in this context, the words hazard and event are used often as synonymous in IAEA SSs and other IAEA publications
- Internal and external hazards have the potential to induce an initiating event and to cause damage to several or many plant equipment or affect plant operation (and even outside emergency response)
- The Internal or the External Hazard is not an initiating event



Design Basis

- **Requirement 17: Internal and external hazards**

All foreseeable internal hazards and external hazards, including the potential for human induced events directly or indirectly to affect the safety of the nuclear power plant, shall be identified and their effects shall be evaluated. Hazards shall be considered in designing the layout of the plant and in determining the postulated initiating events and generated loadings for use in the design of relevant items important to safety for the plant.

- Items important to safety shall be designed and located, with due consideration to other implications for safety, to withstand the effects of hazards or to be protected, according to their importance to safety.

- For multiple unit plant sites, the design shall take due account of the potential for specific hazards to give rise to impacts on several or even all units on the site simultaneously.

Design Basis

- **Requirement 17: Internal and external hazards**

...

External hazards

- The design shall include due consideration of those natural and human induced external events that have been identified in the site evaluation. In the short term, the safety of the plant shall not be permitted to be dependent on the availability of off-site services such as electricity supply and fire fighting services.
- The design of the plant shall provide for an adequate margin to protect items important to safety against hazards taking into account the site hazard evaluation, and to avoid cliff edge effects .
- The design of the plant shall provide for an adequate margin to protect items ultimately necessary to prevent large or early radioactive releases in the event of levels of natural hazards exceeding those to be considered for design taking into account the site hazard evaluation.

Design Basis

- **Requirement 18: Engineering design rules**

  The engineering design rules for items important to safety shall be specified and shall comply with the relevant national or international codes and standards and with sound engineering practices, with account taken of their relevance to nuclear power technology.

Design Basis

- **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 nuclear power 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
  – Safety systems are designed with the application of the “single failure criterion”
  – Key plant parameters shall 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.

Design Basis

Requirement 20: Design extension conditions (DECs)

A set of design extension conditions shall be derived on the basis of engineering judgment, 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

- 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 core damage

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

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

66

Design Basis

Safety features for DEC:

- Shall be independent, to the extent practicable, of those used in more frequent accidents;
- Shall be capable of performing in the environmental conditions related to DEC, including severe accidents, where appropriate;
- In particular, the containment and its safety features shall be able to withstand extreme scenarios that include, among other things, melting of the reactor core. These scenarios shall be selected using engineering judgement

The design shall be such that the possibility of plant states arising that could lead to early or to large releases is **‘practically eliminated’**. For DEC, protective measures that are limited in terms of times and areas of application shall be sufficient for the protection of the public, and sufficient time shall be available to take such measures.

(*) 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.

67

Design Basis

- **Requirement 21: Physical separation and independence of safety systems**

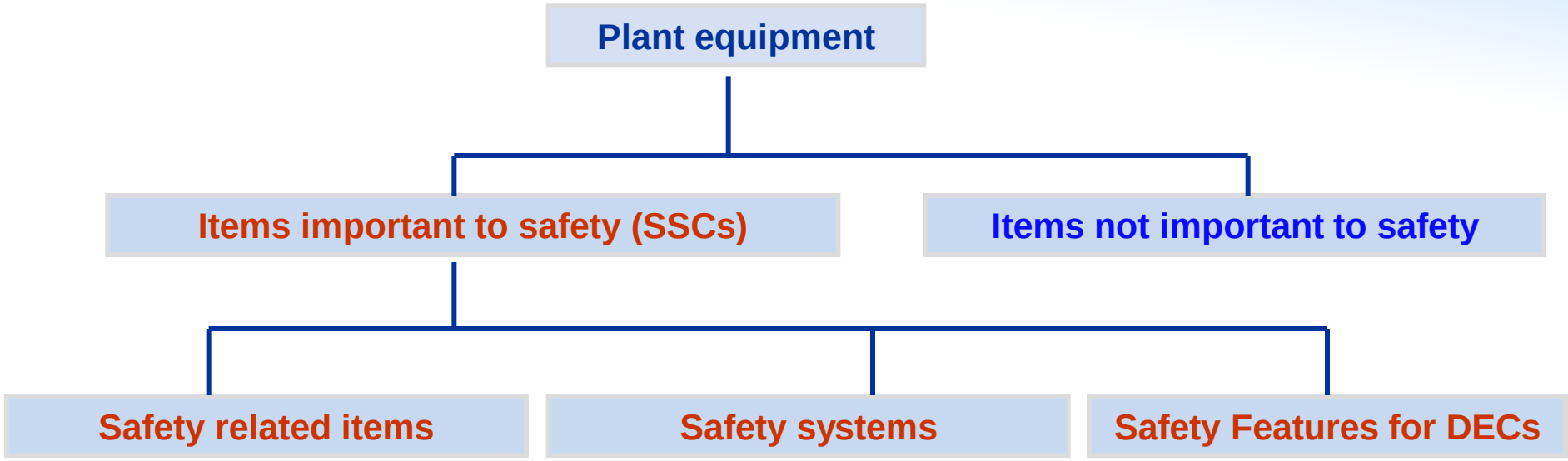
Interference between safety systems or between redundant elements of a system shall be prevented by means such as physical separation, electrical isolation, functional independence and independence of communication (data transfer), as appropriate.

- **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.

- 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: the safety function(s) to be performed by the item; the consequences of failure to perform a safety function; the frequency with which the item will be called upon to perform a safety function, etc.

Plant Equipment Categories



* SSCs = Systems, structures and components

Design Basis

- **Requirement 23: Reliability of items important to safety**

The reliability of items important to safety shall be commensurate with their safety significance.

- **Requirement 24: Common cause failures**

The design of equipment shall take due account of the potential for common cause failures of items important to safety, to determine how the concepts of diversity, redundancy, physical separation and functional independence have to be applied to achieve the necessary reliability.

- **Requirement 25: Single failure criterion**

The single failure criterion shall be applied to each safety group incorporated in the plant design.

Design Basis

- **Requirement 26: Fail-safe design**

  The concept of fail-safe design shall be incorporated, as appropriate, into the design of systems and components important to safety.

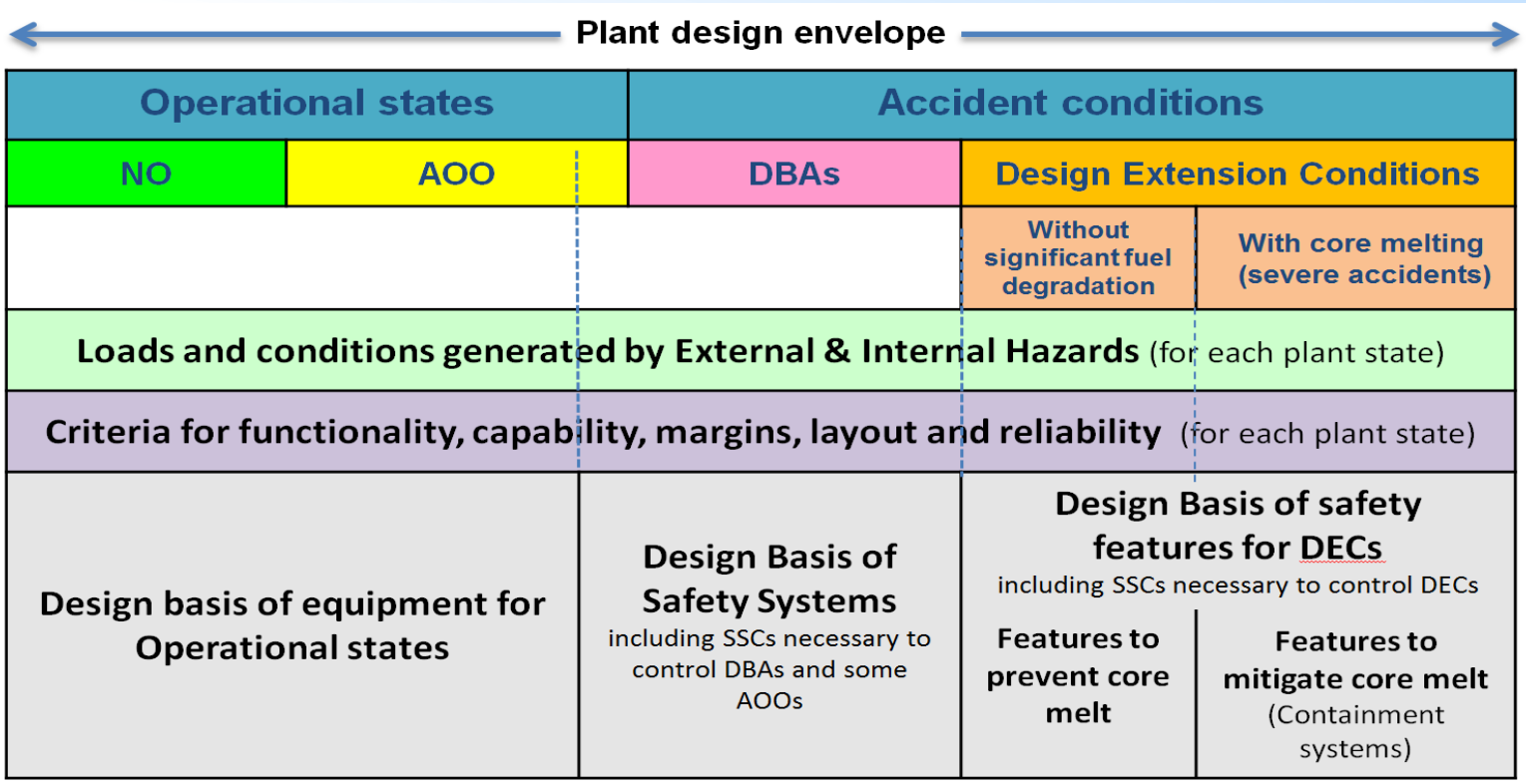
- **Requirement 27: Support service systems**

  Support service systems that ensure the operability of equipment forming part of a system important to safety shall be classified accordingly.

- **Requirement 28: Operational limits and conditions for safe operation**

  The design shall establish a set of operational limits and conditions for safe operation of the nuclear power plant.

Plant Sates & Design Basis



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

Design for the safe operation over the lifetime of the plant

- **Requirement 29: Calibration, testing, maintenance, repair, replacement, inspection and monitoring of items important to safety**

  Items important to safety for a nuclear power plant shall be designed to be calibrated, tested, maintained, repaired or replaced, inspected and monitored as required to ensure their capability of performing their functions and to maintain their integrity in all conditions specified in their design basis.

- **Requirement 30: Qualification of items important to safety**

  A qualification programme for items important to safety shall be implemented to verify that items important to safety at a nuclear power plant are capable of performing their intended functions when necessary, and in the prevailing environmental conditions, throughout their design life, with due account taken of plant conditions during maintenance and testing.

Design for the safe operation over the lifetime of the plant

- **Requirement 31: Ageing management**

  The design life of items important to safety at a nuclear power plant shall be determined. Appropriate margins shall be provided in the design to take due account of relevant mechanisms of ageing, neutron embrittlement and wear out and of the potential for age related degradation, to ensure the capability of items important to safety to perform their necessary safety functions throughout their design life.

Human Factors

- **Requirement 32: Design for optimal operator performance**

  Systematic consideration of human factors, including the human–machine interface, shall be included at an early stage in the design process for a nuclear power plant and shall be continued throughout the entire design process.

Other design considerations

- **Requirement 33: Safety systems, and safety features for DEC of units of a multiple unit nuclear power plant**

  Each unit of a multiple unit nuclear power plant shall have its own safety systems and shall have its own safety features for DEC. To further enhance safety, means allowing interconnections between units of a multiple unit nuclear power plant shall be considered in the design

- **Requirement 34: Systems containing fissile material or radioactive material**

  All systems in a nuclear power plant that could contain fissile material or radioactive material shall be so designed as: to prevent the occurrence of events that could lead to an uncontrolled radioactive release to the environment; to prevent accidental criticality and overheating; …

Safety Analysis

- **Requirement 42: Safety analysis of the plant design**

  A safety analysis of the design for the nuclear power plant shall be conducted in which methods of both deterministic analysis and probabilistic analysis shall be applied to enable the challenges to safety in the various categories of plant states to be evaluated and assessed.

  – On the basis of a safety analysis, the design basis for items important to safety and their links to initiating events and event sequences shall be confirmed. It shall be demonstrated that the nuclear power plant as designed is capable of complying with authorized limits on discharges with regard to radioactive releases and with the dose limits in all operational states, and is capable of meeting acceptable limits for accident conditions.

  – The safety analysis shall provide assurance that defence in depth has been implemented in the design of the plant.

  – The safety analysis shall provide assurance that uncertainties have been given adequate consideration in the design of the plant and in particular that adequate margins are available to avoid cliff edge effects and early radioactive releases or large radioactive releases.

  – The applicability of the analytical assumptions, methods and degree of conservatism used in the design of the plant shall be updated and verified for the current or as built design.

- **Sections 1-2 :** Introduction, Principles and Concepts
- **Section 3 :** Requirements on Management of Safety in design
- **Sections 4:** Principal Technical Requirements
- **Sections 5:** General Plant Design.
- **Section 6:** Requirements for specific plant systems e.g.:

  Reactor core, Reactor coolant systems, Containment systems, I&C, Emergency power supply, fuel handling and storage systems

  REQUIREMENTS 43-80

Design Requirements for:

- Reactor core and associated features
- Reactor coolant systems
- Containment structure and containment systems
- Instrumentation and control systems
- Emergency power supply
- Spent fuel storage and handling
- Other systems