IAEA 60 Years
Atoms for Peace and Development

IAEA Safety Standards SSR-2/1: Safety of Nuclear Power Plants – Design

Simone Massara
Safety Assessment Section
Division of Nuclear Installation Safety
Department of Nuclear Safety and Security

ANSN Workshop on Safety Review and Assessment for Licensing NPPs
Daejeon, Republic of Korea, 27-31 May 2019

Learning objectives

Upon completion of this session, participants will be able to understand the most relevant aspects of the new IAEA Safety Requirements for the Design of Nuclear Power Plants, including:

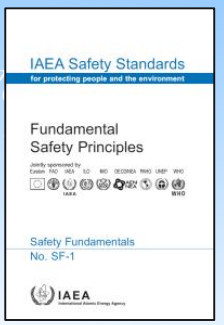
- **Principal technical requirements**, e.g.
  - **Defence in Depth** and its implementation in the design
  - The **extended plant design envelope**
- **General plant design requirements** and safety principles underpinning the NPP design and safety demonstration, e.g.
  - The concept of **practical elimination** of sequences leading to an early or a large radioactive release

Outline

- Introduction: Nuclear Safety Fundamentals
- Generalities on SSR-2/1: Safety of Nuclear Power Plants: Design
- Principal Technical Requirements
  - Extended plant design envelope (including Design Extension Conditions)
  - Defence-in-Depth
- General Plant Design Requirements
  - Practical elimination of sequences leading to early or large radioactive releases
- Design of Specific Plant Systems (examples)
- Inputs for NPP design & licensing
- Conclusions

- Introduction: Nuclear Safety Fundamentals
- Generalities on SSR-2/1: Safety of Nuclear Power Plants: Design
- Principal Technical Requirements
  - Extended plant design envelope (including Design Extension Conditions)
  - Defence-in-Depth
- General Plant Design Requirements
  - Practical elimination of sequences leading to early or large radioactive releases
- Design of Specific Plant Systems (examples)
- Inputs for NPP design & licensing
- Conclusions

Nuclear Safety Fundamentals



From IAEA Safety Standards, Fundamentals Safety Principles, No. SF-1

- **Safety Objective**
  - The fundamental safety objective is to protect people and the environment from harmful effects of ionizing radiation (Chap. 2)
- **Safety**
  - It means the protection of people and the environment against radiation risks, and the safety of facilities and activities that give rise to radiation risks. […] Safety measures include actions to *prevent* incidents and arrangements put in place to *mitigate* their consequences if they were to occur (Chap. 3)

- Introduction: Nuclear Safety Fundamentals
- Generalities on SSR-2/1: Safety of Nuclear Power Plants: Design
- Principal Technical Requirements
  - Extended plant design envelope (including Design Extension Conditions)
  - Defence-in-Depth
- General Plant Design Requirements
  - Practical elimination of sequences leading to early or large radioactive releases
- Design of Specific Plant Systems (examples)
- Inputs for NPP design & licensing
- Conclusions

Safety Standards Hierarchy

Requirements that must be met to ensure protection of people and environment ('shall')

Safety Standards Structure

IAEA 60 Years Atoms for Peace and Development

Safety Fundamentals
Fundamental Safety Principles

General Safety Requirements

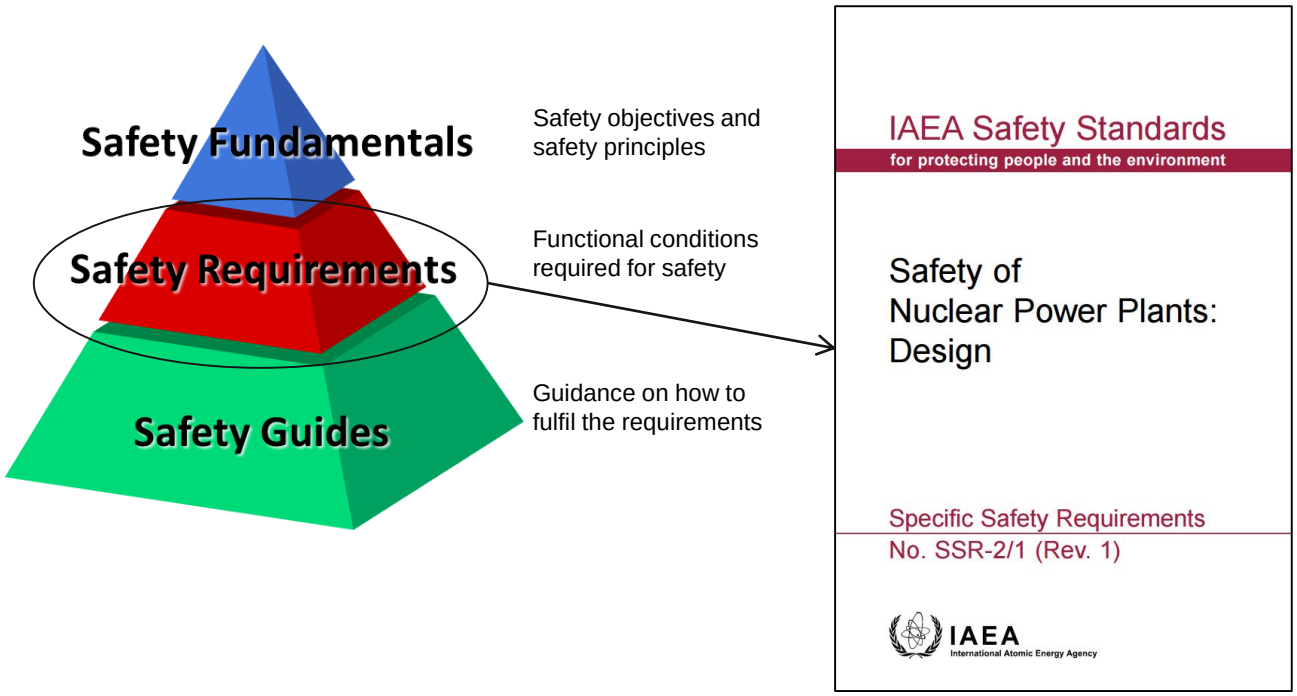
- Part 1. Governmental, Legal and Regulatory Framework for Safety
- Part 2. Leadership and Management for Safety
- Part 3. Radiation Protection and Safety of Radiation Sources
- Part 4. Safety Assessment for Facilities and Activities
- Part 5. Predisposal Management of Radioactive Waste
- Part 6. Decommissioning and Termination of Activities
- Part 7. Emergency Preparedness and Response

Specific Safety Requirements

- 1. Site Evaluation for Nuclear Installations
- 2. Safety of Nuclear Power Plants
  2.1 Design
  2.2 Commissioning and Operation
- 3. Safety of Research Reactors
- 4. Safety of Nuclear Fuel Cycle Facilities
- 5. Safety of Radioactive Waste Disposal Facilities
- 6. Safe Transport of Nuclear Material

Collection of Safety Guides

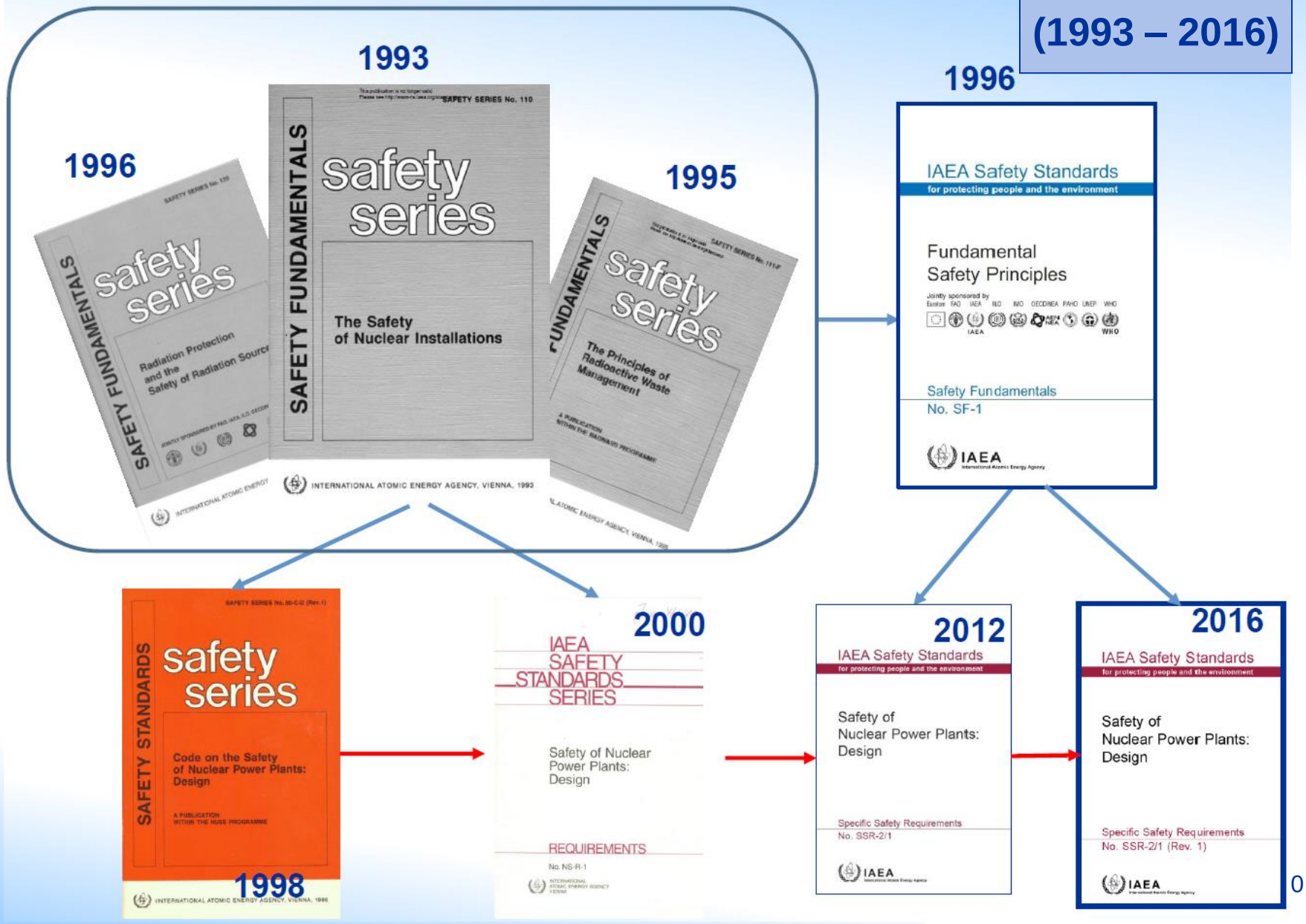
Design Safety



- 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 (**Regulatory Body**) to assess the safety of a given NPP design

Design Safety: Historical view… over 20+ years

(1993 – 2016)



IAEA follow-up to publication of SSR-2/1 (Rev. 0)

- IAEA Commission on Safety Standards (CSS) asked for the IAEA to initiate the revision of SSR-2/1, together with other SSR and SG to include lessons learnt from Fukushima-Daiichi accident: **SSR-2/1 (Rev. 1) will be published in 2016**
- IAEA Technical Secretariat initiated the development of TECDOC-1791 (eventually published in 2016)
  - Aimed at facilitating a common interpretation and implementation of new requirements by MS
  - While facilitating and harmonizing the revision/preparation of new safety guides for design and safety assessment of NPPs

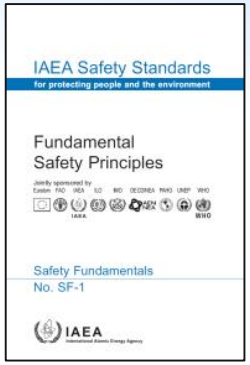
CONTENTS

Relevant Safety Guides

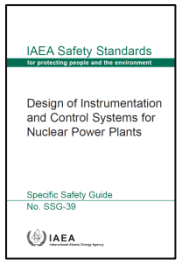
Safety objectives and safety principles

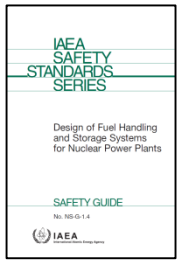
Functional conditions required for safety

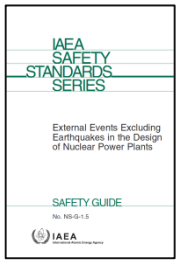
Guidance on how to fulfil the requirements

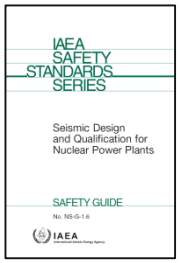


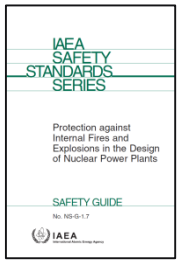
- Design of specific systems
- General design aspects

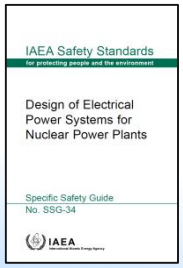


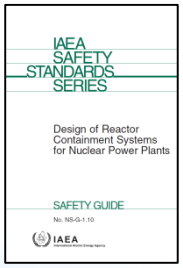


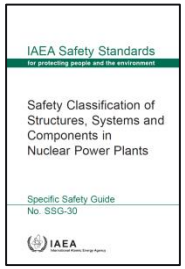


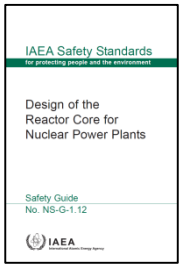


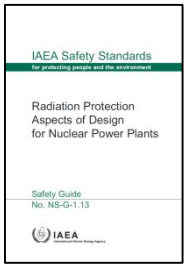


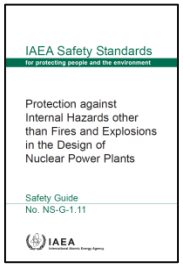










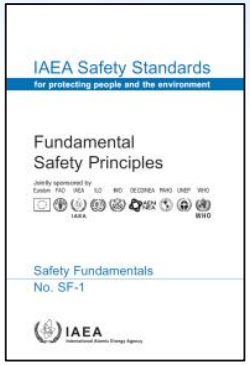


Relevant Safety Guides under revision

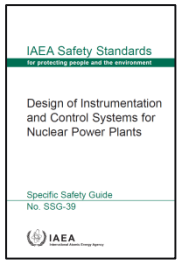
Safety objectives and safety principles

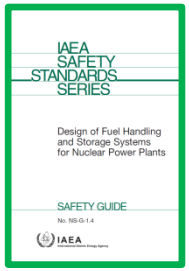
Functional conditions required for safety

Guidance on how to fulfil the requirements

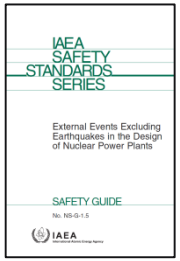


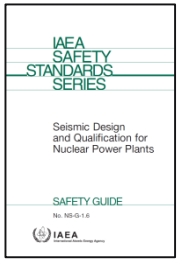
- Design of specific systems
- General design aspects

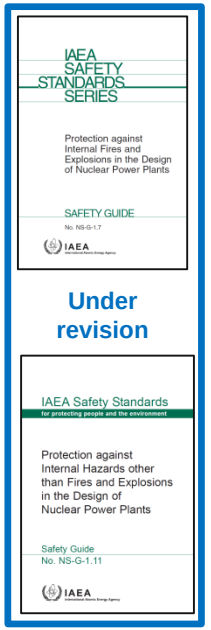




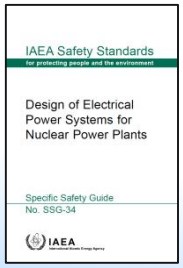
Rev. 1 soon available

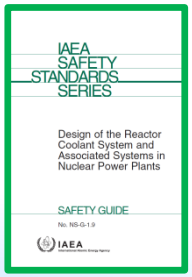




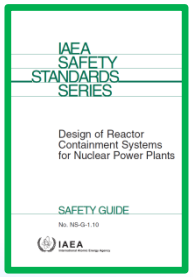


Under revision

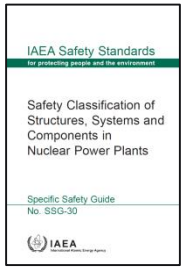


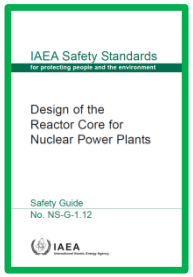


Rev. 1 soon available

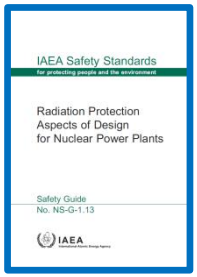


Rev. 1 soon available





Rev. 1 soon available



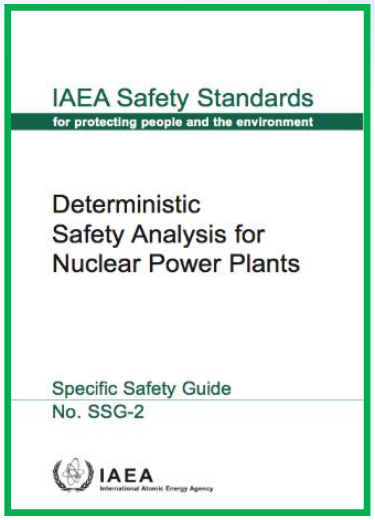
Under revision

Relevant Safety Guides under revision

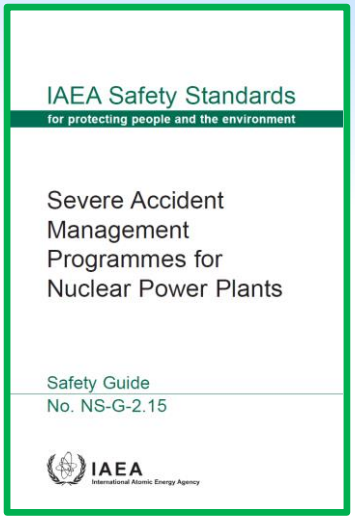
Safety objectives and safety principles

Functional conditions required for safety

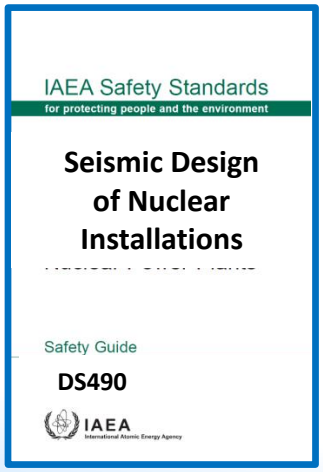
Guidance on how to fulfil the requirements



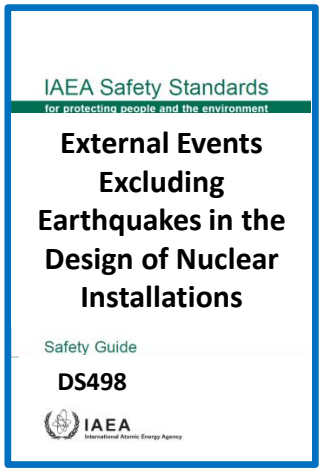
Rev. 1 soon available



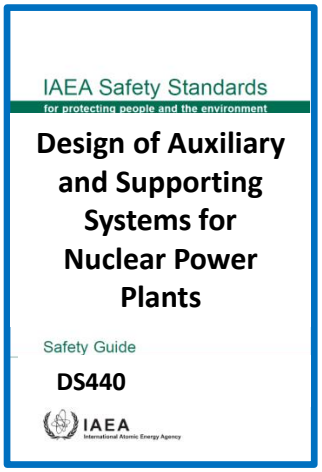
Rev. 1 soon available



Under revision



Under revision



Under revision

Revision of SSR-2/1 (2016): Overview

- Reinforcement of Defence-in-Depth (**DiD)** and 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 of **non-permanent equipment for accident management**
- Reinforced capabilities for **power supply in DECs**
- Additional measures for **spent fuel pool** instrumentation, cooling and maintaining inventory

Applicability of SSR-2/1 (Rev. 1)

- **Primarily: land based stationary NPPs with water cooled reactors**
- With judgement: for application to **other reactor types**, to determine how the requirements have to be considered in developing the design
- For **NPPs already in operation:**
  - It might not be practicable to apply all requirements
  - It is expected that a comparison will be made against the current standards, for example as part of the periodic safety review for a plant

Importance of Requirements for NPP Design

- Define the **safety approach** for NPP design
  - Reflect current technologies and good practices, as well as views and licensing practices of IAEA MS
  - Consensus document
- Significantly contributed to establishing a **common safety approach and terminology**
- Main reference to perform **IAEA design safety reviews**
- **Reference** for establishing/complementing **licensing regulations** in several countries

SSR-2/1: Structure

- **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.

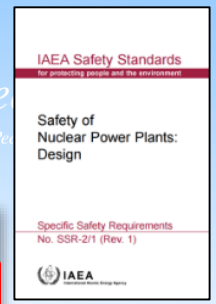
SSR-2/1: Table of contents

- INTRODUCTION
- APPLYING SAFETY PRINCIPLES AND CONCEPTS
- 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)

Safety objectives; Radiation protection; Defence in depth

82 requirements

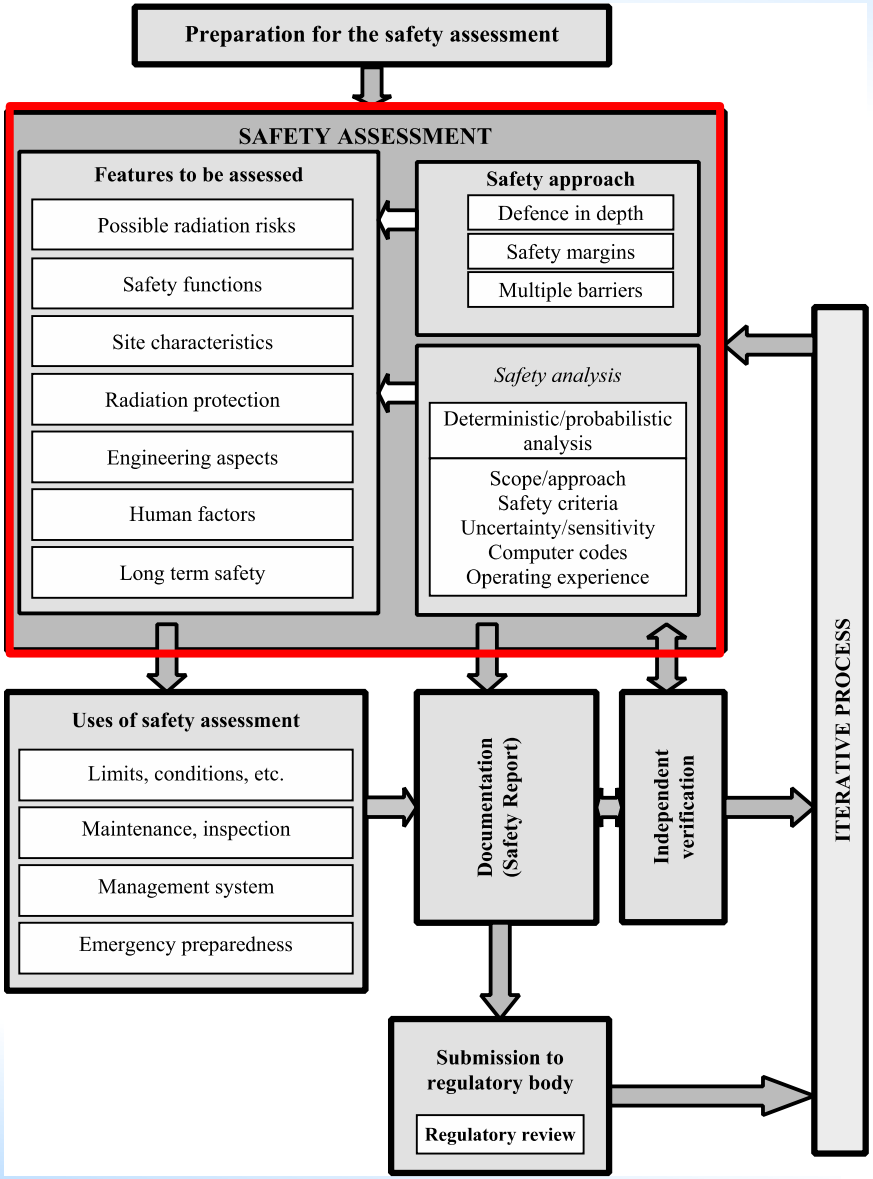
SSR-2/1: Table of contents (1 / 2)

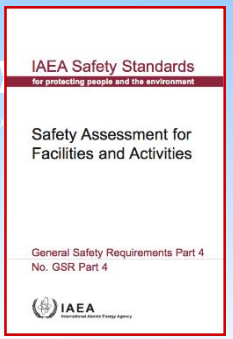


CONTENTS

SSR-2/1: Table of contents (2 / 2)

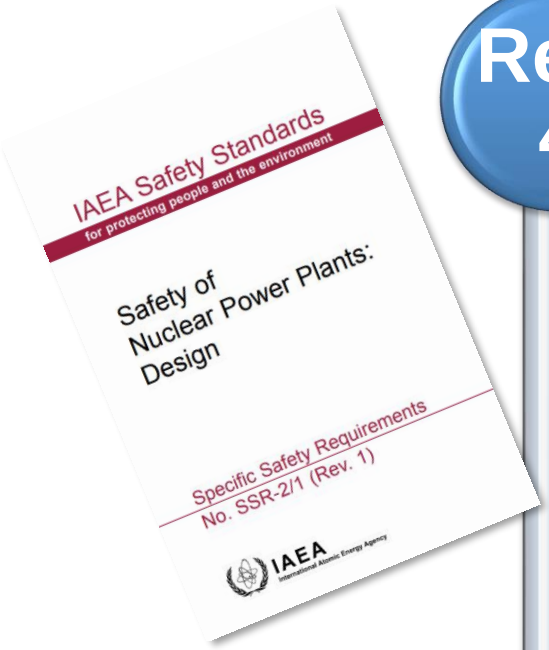
GSR-4: Safety assessment





- Introduction: Nuclear Safety Fundamentals
- Generalities on SSR-2/1: Safety of Nuclear Power Plants: Design
- Principal Technical Requirements
  - Extended plant design envelope (including Design Extension Conditions)
  - Defence-in-Depth
- General Plant Design Requirements
  - Practical elimination of sequences leading to early or large radioactive releases
- Design of Specific Plant Systems (examples)
- Inputs for NPP design & licensing
- Conclusions

SSR-2/1 Principal Technical Requirements



Req. 4

FUNDAMENTAL SAFETY FUNCTIONS

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**

Fundamental safety functions

Control of reactivity

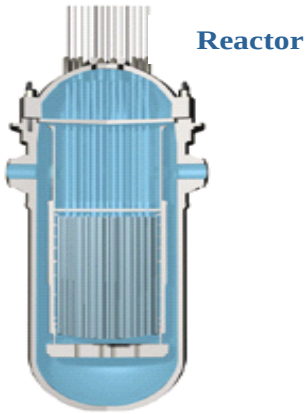
- Control rods
- Boron concentration

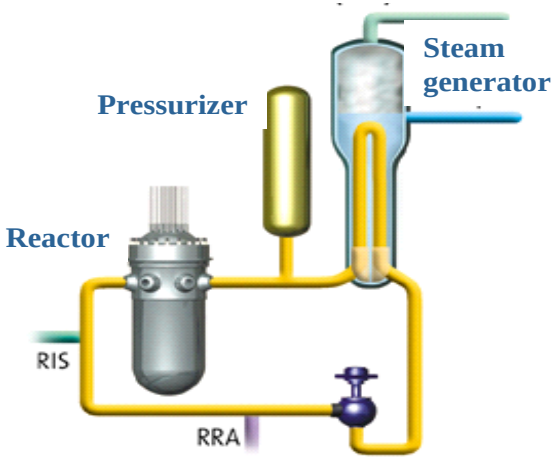
Cooling of the core

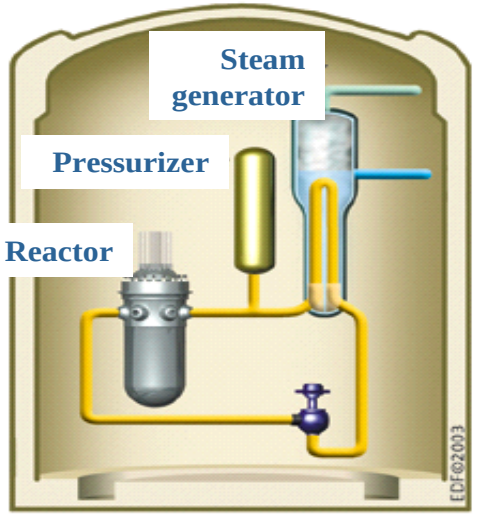
- Steam generators
- RHR
- Safety injection
- …

Confinement of radioactive materials

- Fuel cladding (1st barrier)
- Primary cooling system (2nd)
- Containment (3rd)







Fuel cladding and reactor core accomplish key safety functions and constitute the first two barriers (cladding, primary system) for the confinement of radioactive elements, the third barrier being the containment

Updated plant states definition within SSR-2/1

Req. 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.

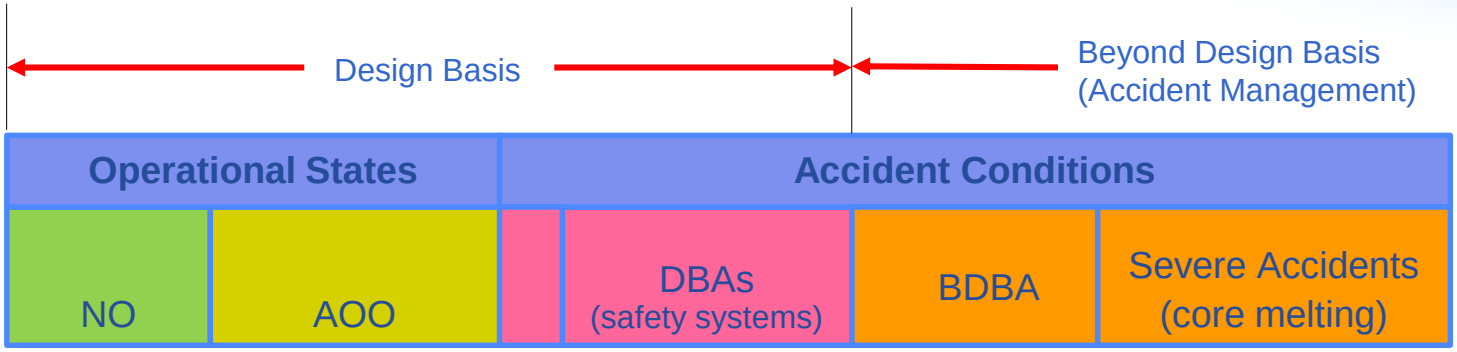
- **Normal operation**;
- **Anticipated operational occurrences**, which are expected to occur over the operating lifetime of the plant;
- **Design basis accidents**;
- **Design extension conditions**, including accidents without and with core melting.

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.

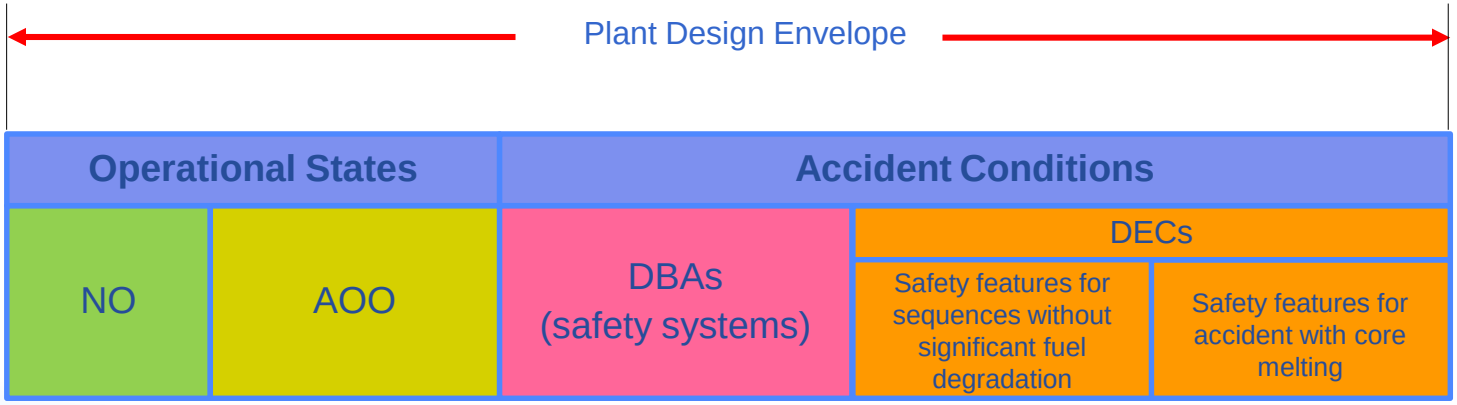
Operational states		Accident conditions		Large or Early Releases
Normal Operation NO	Anticipated Operational Occurrences AOO	Design Basis Accidents DBA	Design Extension Conditions DEC	Practically Eliminated

New Design Safety Principles

Earlier Concept



SSR-2/1, 2012



Conditions practically eliminated

SF-1 Safety Principle 8: Prevention of Accidents

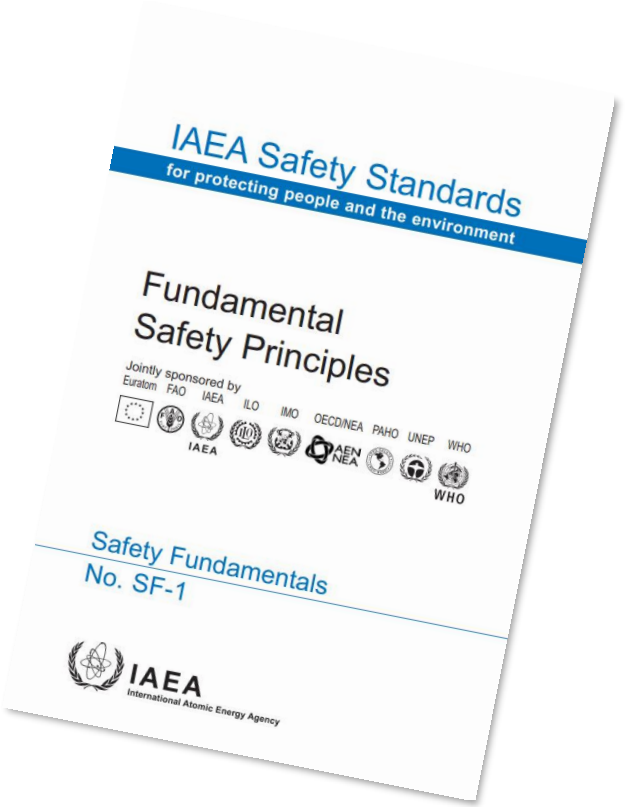
All practical efforts must be made to prevent and mitigate nuclear or radiation accidents

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*



Overview of the DiD concept

- The concept of DiD is fundamental to the safety of nuclear installations and should be broadly applied by designer and utility organizations in all activities dealing with design and operation of nuclear installations

- DiD provides a hierarchical deployment of different independent levels of equipment and procedures in order to maintain the effectiveness of physical barriers placed between radioactive materials, the workers, public, and the environment, during normal operation and potential accident conditions

Summary of historical development

1988 – INSAG-3, Basic Safety Principles for NPPs:
The concept of DiD outlined

1996 – INSAG-10, DiD in Nuclear Safety:
Objectives, strategy, implementation

1999 – INSAG-12 (update of INSAG-3):
The central concept is DiD

2000-2005 – IAEA Safety Standards*: DiD emphasized*

2005 – Safety Reports Series No. 46, Assessment of DiD for NPPs: *A method for assessing the defence in depth capabilities*

2006 – An extensive program on revision of the existing and development of new IAEA Safety Standards started:
DiD re-emphasized

DiD: 1st Level

Prevention of abnormal operation and failures of items important to safety.

- Sound and conservative siting, design (adequate margins), maintenance and operation in accordance with quality management and appropriate and proven engineering practices
- Selection of appropriate design codes and materials, and to the quality control of the manufacture of components, construction and commissioning of the plant
- Use of design options that reduce the potential for internal hazards
- Provisions and processes for design, manufacture, construction and in-service inspection, maintenance and testing
- Comprehensive training of appropriately selected operating personnel whose behaviour is consistent with a sound safety culture
- Adequate time for operators to respond to events and appropriate human-machine interfaces
- Operating instructions and monitoring of plant status and operating conditions
- Recording, evaluation and utilization of operating experience

DiD: 2nd Level

Detection and control of deviations from normal operational states to prevent Anticipated Operational Occurrences at the plant from escalating to accident conditions

- Intrinsic plant characteristics (core stability, thermal inertia, etc.)
- Limitation and Protection systems. Other automatic actions
- Specific systems and features in the design to return the plant to a safe state.
- Control room alarms
- Procedures to prevent anticipated operational occurrences, or otherwise to minimize their consequences.

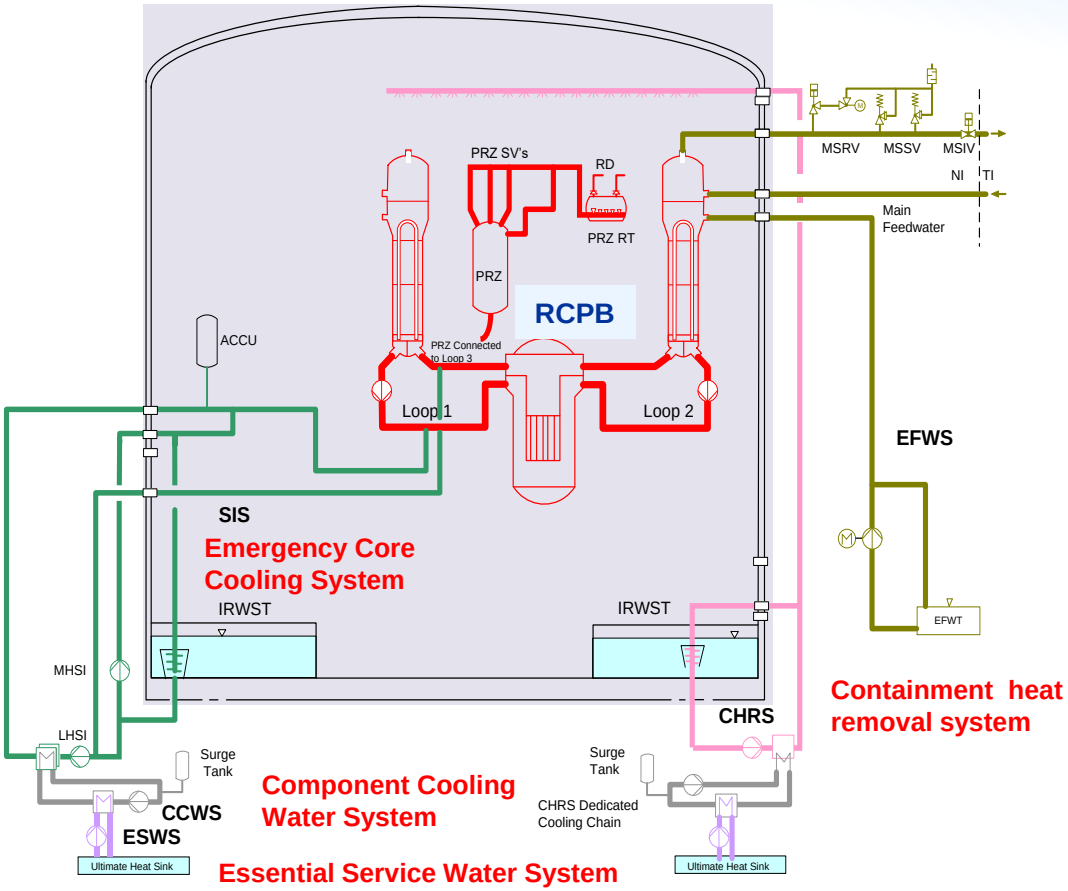
DiD: 3rd Level

Mitigation of accidents.
Prevention of severe accidents.

- Inherent and/or engineered safety features, safety systems and procedures be capable of preventing damage to the reactor core
- Measures applied to ensure a high reliability of safety systems:
  - Redundancy and diversity
  - Physical separation
  - Automatic actuations
  - Adequate classification of structures, systems and components (SSCs)
  - Testing capability

DiD: 3rd Level

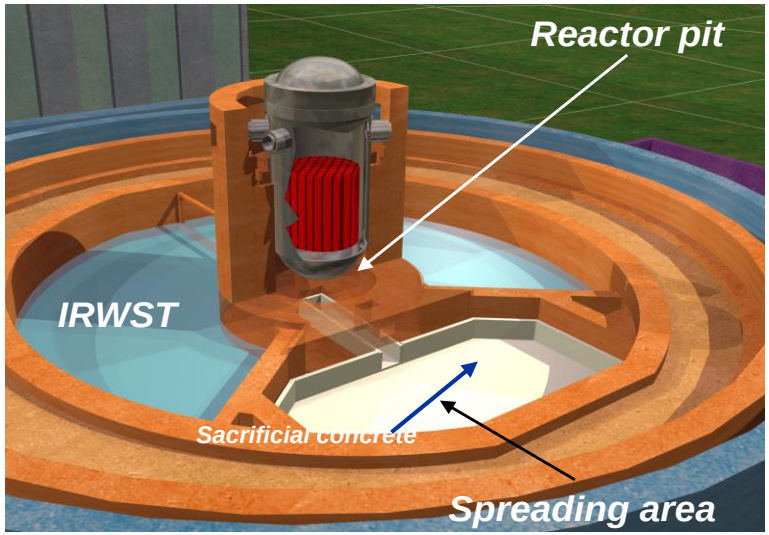
Examples of Safety Systems



DiD: 4th Level

Control of severe plant conditions.
Mitigation of severe accident consequences.

- First objective is to protect the containment to prevent releases
  - Containment cooling
  - Containment isolation
  - Hydrogen control
  - Other systems for severe accidents:
    - In/ex vessel retention
    - Containment venting
  - Accident management (SAMG)



- Event sequences that would lead to an early radioactive release or a large radioactive release are required to be 'practically eliminated'

DiD: 5th Level

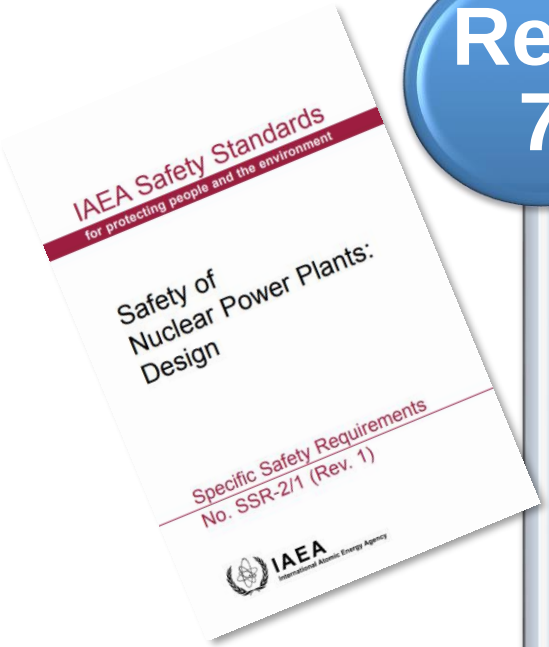
Mitigation of off-site radiological consequences

- Emergency off-site plans and procedures
- Both on-site and off-site emergency plans are exercised periodically

Summary of DiD levels

Level of defence Approach 1	Objective	Essential design means	Essential operational means	Level of defence Approach 2
Level 1	Prevention of abnormal operation and failures	Conservative design and high quality in construction of normal operation systems, including monitoring and control systems	Operational rules and normal operating procedures	Level 1
Level 2	Control of abnormal operation and detection of failures	Limitation and protection systems and other surveillance features	Abnormal operating procedures/emergency operating procedures	Level 2
3a Level 3	Control of design basis accidents (postulated single initiating events)	Engineered safety features (safety systems)	Emergency operating procedures	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. Technical Support Centre	Complementary emergency operating procedures/ severe accident management guidelines	Level 4 4b
Level 5	Mitigation of radiological consequences of significant releases of radioactive materials	On-site and off-site emergency response facilities	On-site and off-site emergency plans	Level 5

SSR-2/1 Principal Technical Requirements



Req. 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

SSR-2/1 Principal Technical Requirements

Req. 7

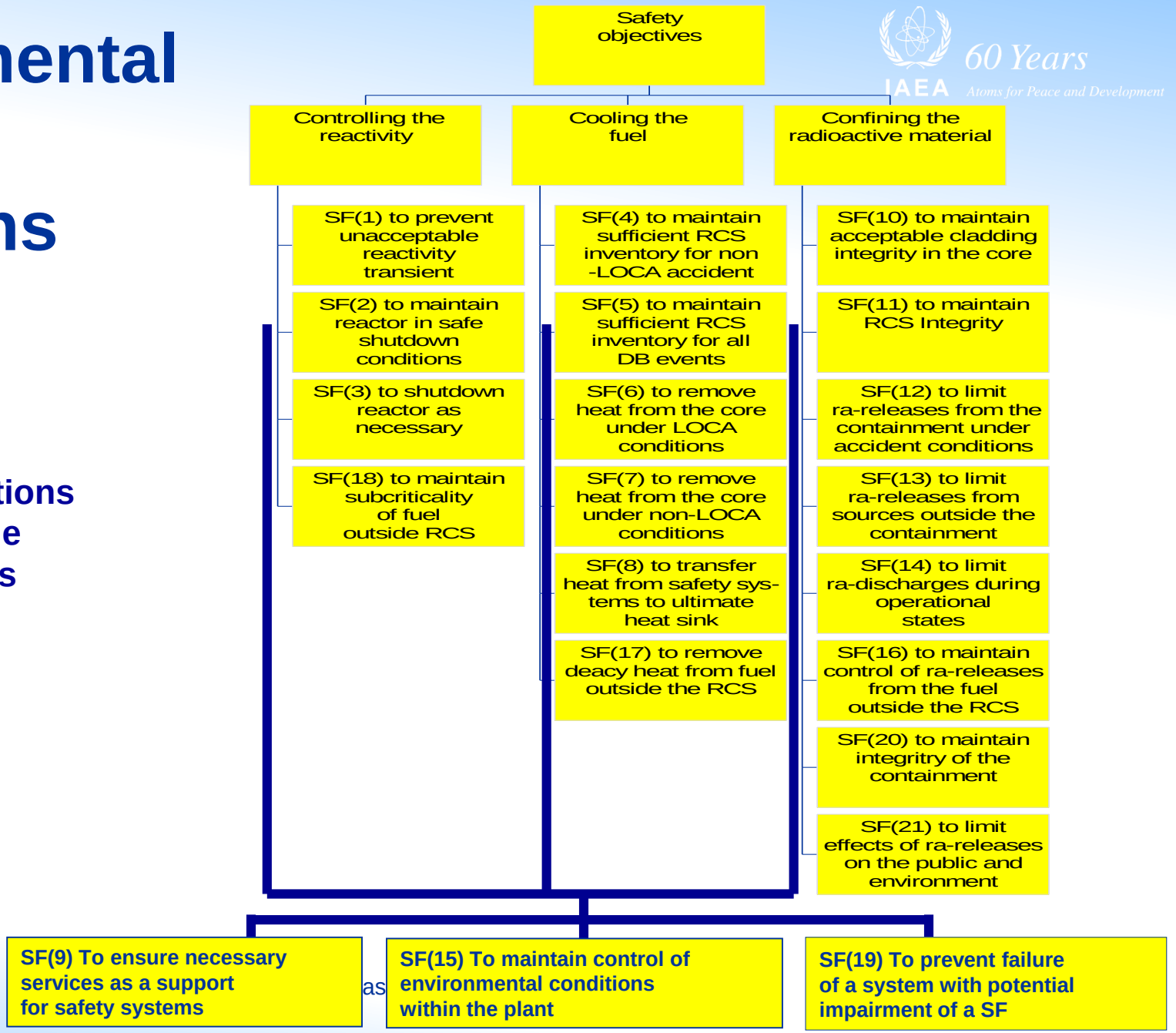
[…]

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

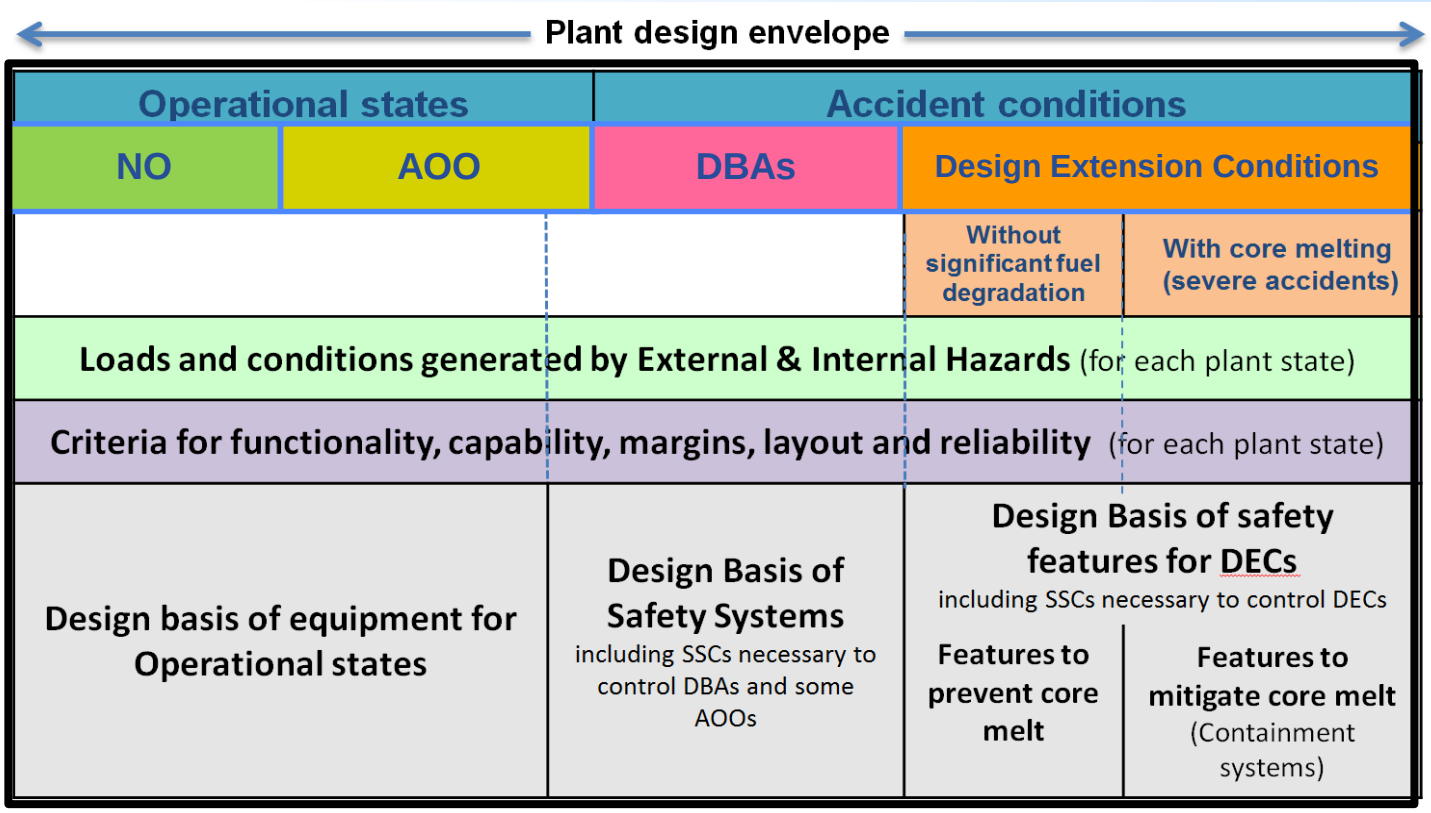
Fundamental safety functions

Safety functions applicable for LWRs



- Introduction: Nuclear Safety Fundamentals
- Generalities on SSR-2/1: Safety of Nuclear Power Plants: Design
- Principal Technical Requirements
  - Extended plant design envelope (including Design Extension Conditions)
  - Defence-in-Depth
- General Plant Design Requirements
  - Practical elimination of sequences leading to early or large radioactive releases
- Design of Specific Plant Systems (examples)
- Inputs for NPP design & licensing
- Conclusions

Plant States & Design Basis



The **design basis** identifies for each **Structure, System and Component (SSC)**:

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

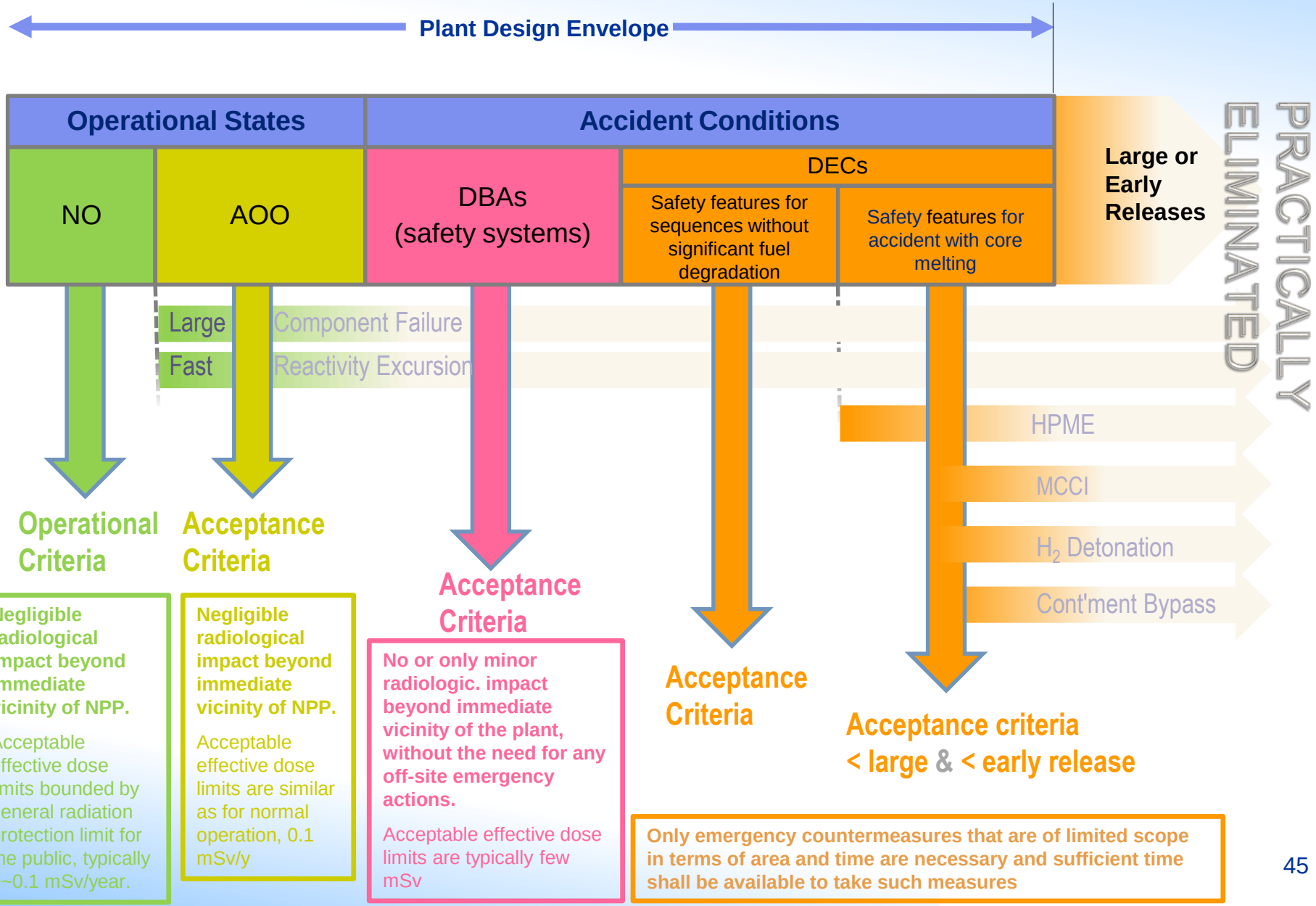
SSR-2/1 General Plant Design

- **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

Updated Safety Demonstration



Practical Elimination

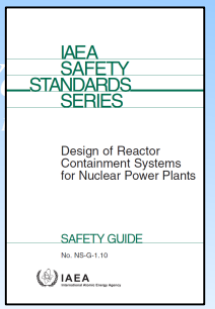
IAEA SSR-2/1

*"**Req. 20**. 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"*

- The term was already introduced in **INSAG 12 (1990)** and in the **IAEA Safety Standards (NS-G-1.10 on Containment)** in **2004**
- The '**certain conditions**' to be addressed referred to hypothetical accident sequences that could lead to early or large radioactive releases due to containment failure than can not be mitigated with implementation of reasonable technical means

Practical Elimination



- **NS-G-1.10: DESIGN CONSIDERATIONS FOR SEVERE ACCIDENTS**

6.5. For new plants, possible severe accidents should be considered at the design stage of the containment systems. The consideration of severe accidents should be aimed at practically eliminating[14] the following conditions:

- Severe accident conditions that could damage the containment in an early phase as a result of direct containment heating, steam explosion or hydrogen detonation;
- Severe accident conditions that could damage the containment in a late phase as a result of basemat melt-through or containment overpressurization;
- Severe accident conditions with an open containment, notably in shutdown states;
- Severe accident conditions with containment bypass, such as conditions relating to the rupture of a steam generator tube or an interfacing system LOCA.

6.6. For severe accidents that cannot be practically eliminated, the containment systems should be capable of contributing to the reduction of the radioactive releases to such a level that the extent of any necessary off-site emergency measures needed is minimal.

NS-G-1.10 Footnote 14 p. 72:
In this context, 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.

Practical Elimination

- **SSR-2/1: SAFETY IN DESIGN**

  2.11. […] Plant event sequences that could result in high radiation doses or in a large radioactive release have to be 'practically eliminated'[2] and plant event sequences with a significant frequency of occurrence have to have no, or only minor, potential radiological consequences. […]

- **SSR-2/1: THE CONCEPT OF DEFENCE IN DEPTH**

  2.13. […] 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 such accidents and mitigating the consequences of a severe accident. The safety objective in the case of a severe accident is that only protective actions that are limited in terms of lengths of time and areas of application would be necessary and that off-site contamination would be avoided or minimized. Event sequences that would lead to an early radioactive release or a large radioactive release[3] are required to be 'practically eliminated'[4].

New in Rev.1

SSR-2/1 Footnote 3: An 'early radioactive release' in this context is a radioactive release for which off-site protective actions would be necessary but would be unlikely to be fully effective in due time. A 'large radioactive release' is a radioactive release for which off-site protective actions that are limited in terms of lengths of time and areas of application would be insufficient for the protection of people and of the environment.

SSR-2/1 Footnote 2 p.6, 4 p.8, 7 p.13, 14 p.24, 16 p.25, 26 p.58 (same as NS-G-1.10)
The possibility of certain conditions arising may be considered to have been 'practically eliminated' if it would be physically impossible for the conditions to arise or if these conditions could be considered with a high level of confidence to be extremely unlikely to arise.

Practical Elimination

- **SSR-2/1 Req. 5: Radiation protection in design**

  […] **4.3.** The design shall be such as to ensure that plant states that could lead to high radiation doses or to a large radioactive release have been 'practically eliminated'[7], and that there would be no, or only minor, potential radiological consequences for plant states with a significant likelihood of occurrence.

- **SSR-2/1 Req. 20: Design Extension Conditions**

  5.27. […] The plant shall be designed so that it can be brought into a controlled state and the containment function can be maintained, with the result that the possibility of plant states arising that could lead to an early radioactive release or a large radioactive release is 'practically eliminated'[14]. […]

  5.31. The design shall be such that the possibility of conditions arising that could lead to an early radioactive release or a large radioactive release is 'practically eliminated' [16].

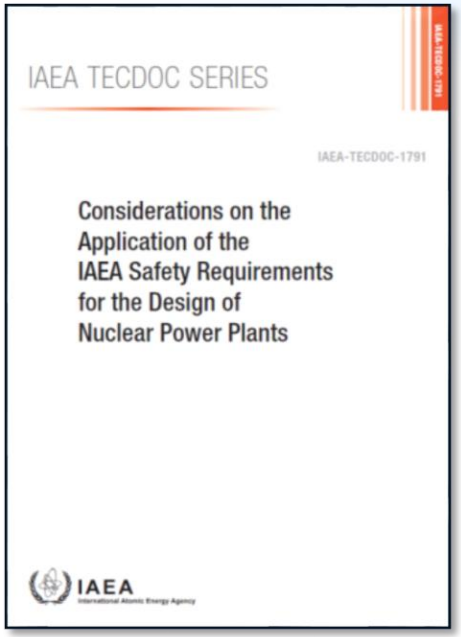
- **SSR-2/1 Req. 80: Fuel handling and storage systems**

  […] **6.68.** For reactors using a water pool system for fuel storage, the design shall be such as to prevent the uncovering of fuel assemblies in all plant states that are of relevance for the spent fuel pool so that the possibility of conditions arising that could lead to an early radioactive release or a large radioactive release is 'practically eliminated'[26] and so as to avoid high radiation fields on the site.

Conditions to be Practically Eliminated

Hypothetical accident sequences

- Events that could lead to prompt reactor core damage and consequent early containment failure
  - Failure of a large component in the reactor coolant system
  - Uncontrolled reactivity accidents
- Very energetic phenomena in severe accident conditions for which technical solutions for maintaining containment integrity cannot be ensured.
  - Core meltdown at high pressure (Direct Containment Heating)
  - Steam explosion
  - Hydrogen explosion
  - Containment boundary melt-through
  - Containment failure due to fast over-pressurization
- Non confined severe fuel damage
  - Severe accident with containment by-pass
  - Significant fuel failure in a storage pool



Design for the safe operation over the lifetime of the plant

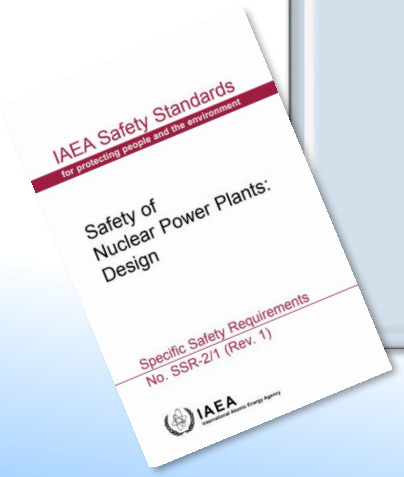
Req. 31

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.

- Design shall take account of ageing and wear out effects in all operational states

- Provisions shall be made for monitoring, testing, sampling and inspections



- Introduction: Nuclear Safety Fundamentals
- Generalities on SSR-2/1: Safety of Nuclear Power Plants: Design
- Principal Technical Requirements
  - Extended plant design envelope (including Design Extension Conditions)
  - Defence-in-Depth
- General Plant Design Requirements
  - Practical elimination of sequences leading to early or large radioactive releases
- Design of Specific Plant Systems (examples)
- Inputs for NPP design & licensing
- Conclusions

Design of Specific Plant Systems

REACTOR CORE AND ASSOCIATED FEATURES

- **Requirement 43: Performance of fuel elements and assemblies**

  Fuel elements and assemblies for the nuclear power plant shall be designed to maintain their structural integrity, and to withstand satisfactorily the anticipated radiation levels and other conditions in the reactor core, in combination with all processes of deterioration that could occur in operational states

- **Requirement 44: Structural capability of the reactor core**

  The fuel elements and fuel assemblies and their supporting structures for the nuclear power plant shall be designed so that, in operational states and in accident conditions other than severe accidents, a geometry that allows for adequate cooling is maintained and the insertion of control rods is not impeded

Design of Specific Plant Systems

REACTOR CORE AND ASSOCIATED FEATURES

- **Requirement 45: Control of the reactor core**

  Distributions of neutron flux that can arise in any state of the reactor core in the nuclear power plant, including states arising after shutdown and during or after refuelling, and states arising from anticipated operational occurrences and from accident conditions not involving degradation of the reactor core, shall be inherently stable

- **Requirement 46: Reactor shutdown**

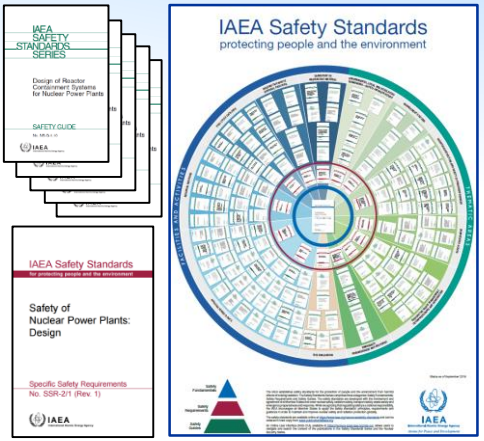
  Means shall be provided to ensure that there is a capability to shut down the reactor of the nuclear power plant in operational states and in accident conditions, and that the shutdown condition can be maintained even for the most reactive conditions of the reactor core.

  – The means for shutting down the reactor shall consist of at least two diverse and independent systems

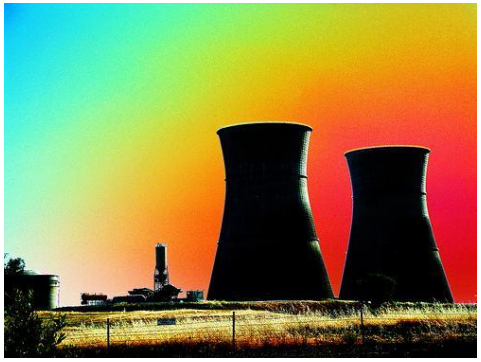
  – At least one of the two different shutdown systems shall be capable, on its own, of maintaining the reactor subcritical by an adequate margin and with high reliability, even for the most reactive conditions of the reactor core

- Introduction: Nuclear Safety Fundamentals
- Generalities on SSR-2/1: Safety of Nuclear Power Plants: Design
- Principal Technical Requirements
  - Extended plant design envelope (including Design Extension Conditions)
  - Defence-in-Depth
- General Plant Design Requirements
  - Practical elimination of sequences leading to early or large radioactive releases
- Design of Specific Plant Systems (examples)
- Inputs for NPP design & licensing
- Conclusions

Inputs for NPP Design & Licensing



National legislations



Industrial Codes & Standards

Western European WENRA Nuclear Regulators' Association

EU Nuclear Safety Directive art. 8a

ENSREG European Nuclear Safety Regulators Group

World Nuclear Association

CORDEL

OECD BETTER POLICIES FOR BETTER LIVES

AEN NEA

MDEP Multinational Design Evaluation Programme

EUR

ENISS

EPRI Utility Requirements Document

- Introduction: Nuclear Safety Fundamentals
- Generalities on SSR-2/1: Safety of Nuclear Power Plants: Design
- Principal Technical Requirements
  - Extended plant design envelope (including Design Extension Conditions)
  - Defence-in-Depth
- General Plant Design Requirements
  - Practical elimination of sequences leading to early or large radioactive releases
- Design of Specific Plant Systems (examples)
- Inputs for NPP design & licensing
- Conclusions

Conclusions

- IAEA SSR-2/1 reflects an **international consensus** on what constitutes a **high level of safety**, pertaining to the requirements for the design of NPPs
- It is intended for use by:
  - **Organisations** involved in design, manufacture, construction, modification, maintenance, operation and decommissioning for NPPs
  - In **analysis**, verification and review, and in the provision of technical support, as well as by regulatory bodies

…Thank you for your attention

S.Massara@iaea.org