

# OVERVIEW OF IAEA DESIGN SAFETY REQUIREMENTS FOR NUCLEAR POWER PLANTS

11th International School on Nuclear Power  
Warsaw, Poland, *May 15 – 18, 2023*

**Jorge LUIS HERNANDEZ**

Safety Assessment Section (SAS)

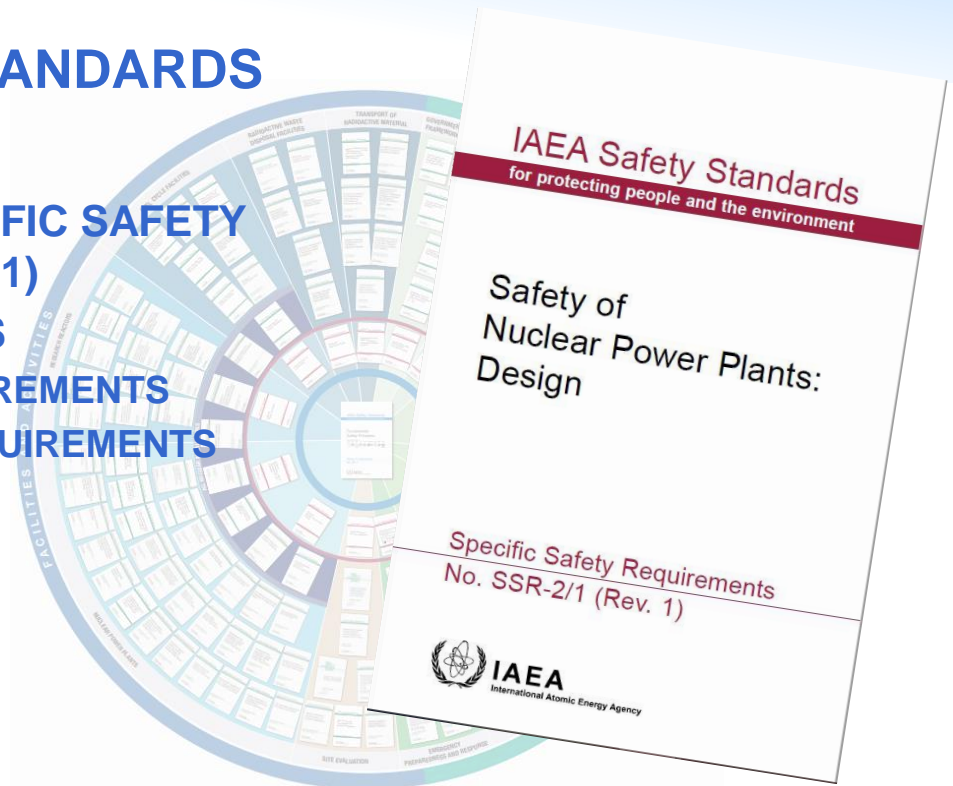
Division of Nuclear Installation Safety (NSNI)

Department of Nuclear Safety and Security (NS)

International Atomic Energy Agency (IAEA)

# Outline

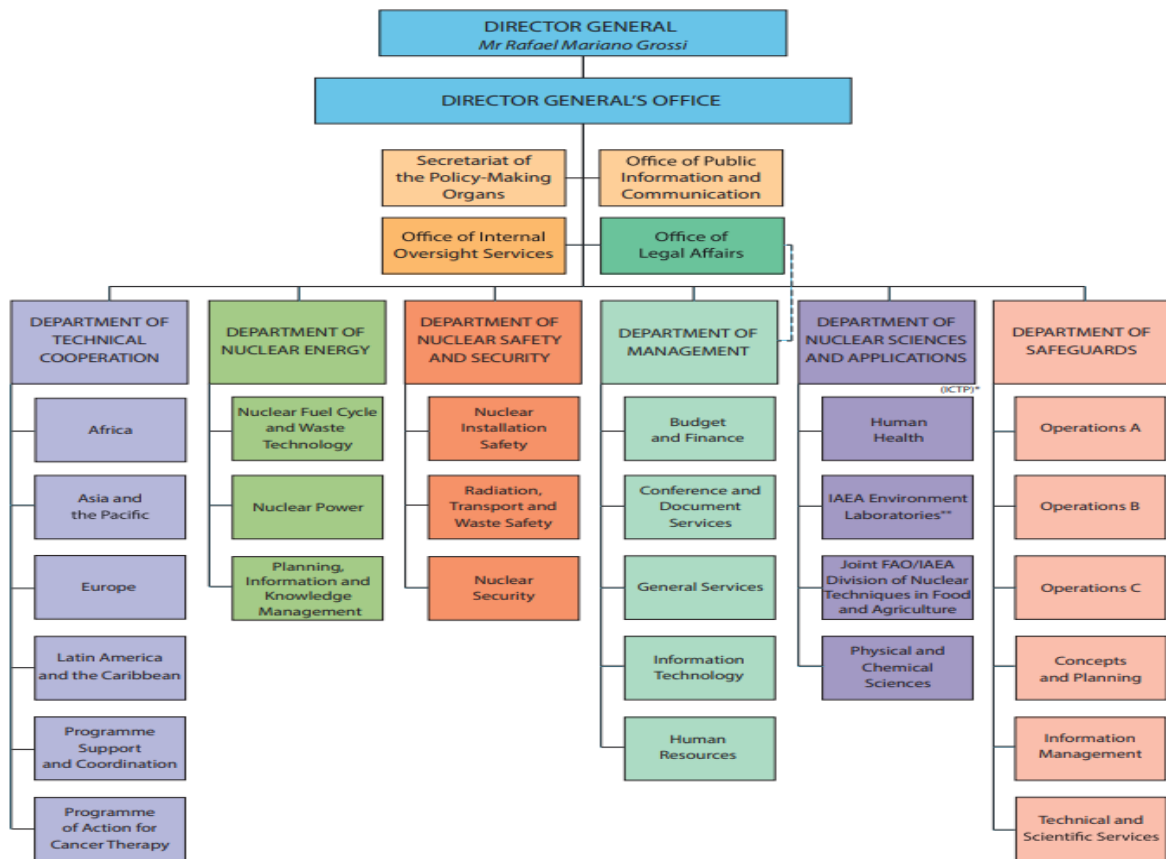
- INTRODUCTION TO SAFETY ASSESSMENT SECTION
- INTRODUCTION TO SAFETY STANDARDS
- DESIGN SAFETY
  - INTRODUCTION TO IAEA SPECIFIC SAFETY REQUIREMENTS SSR-2/1 (REV. 1)
  - OVERVIEW OF REQUIREMENTS
    - PRINCIPAL TECHNICAL REQUIREMENTS
    - GENERAL PLANT DESIGN REQUIREMENTS
- CONCLUSIONS



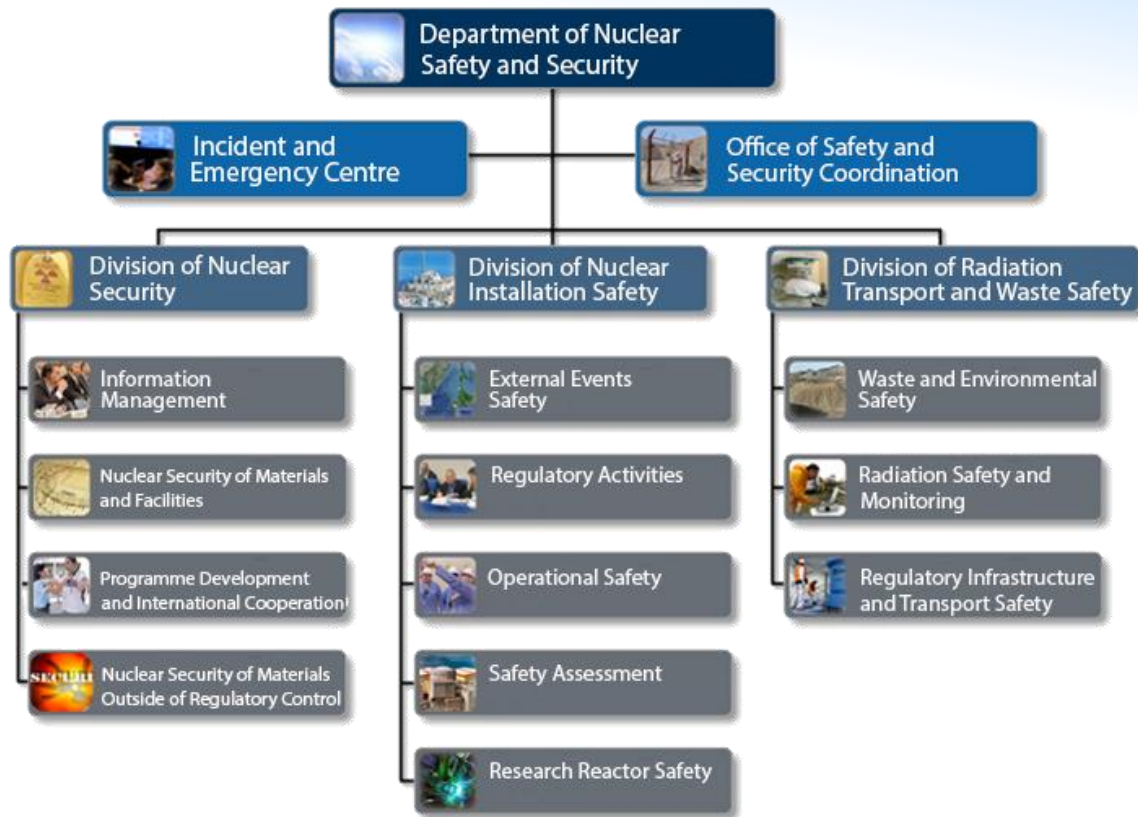
# **Nuclear Installation Safety**

## **Safety Assessment Section**

# IAEA Organizational Structure & NSNI



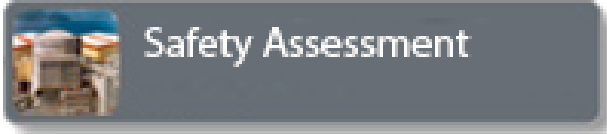
# Safety Assessment Section





- To support Member States
  - in establishing the appropriate safety infrastructure
  - to continuously improve the safety of nuclear installations
    - site evaluation
    - design
    - construction
    - operation
  - through the development of up-to-date safety standards and providing assistance for their effective application.

# Safety Assessment Section Mission & Objectives



**Mission:** To support Member States in achieving a high level of safety in nuclear power plant design and excellence in safety assessment.

## **Objectives:**

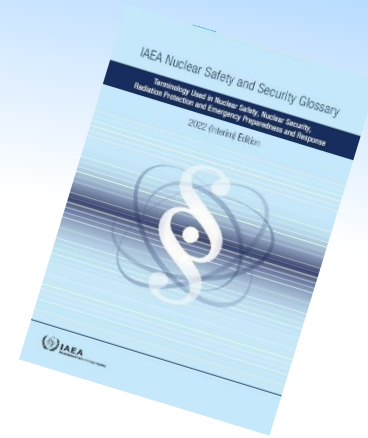
- To provide Member States (MSs) with up-to-date safety assessment and design safety standards based on current technology and best practices
- To support MSs with advice and review services in the implementation of safety assessment and design safety standards
- To develop safety assessment knowledge requirements and provide support to MSs in safety assessment competency and capacity building



# What is nuclear safety?



# What is nuclear safety?

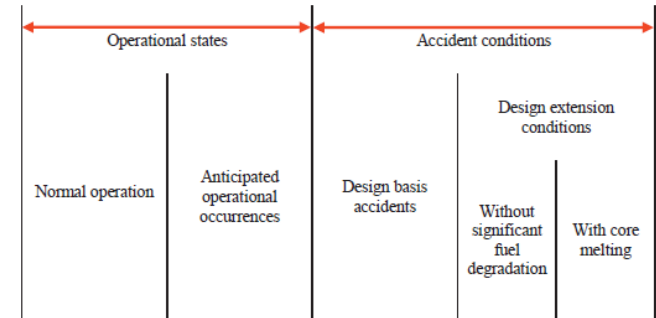


(nuclear) safety

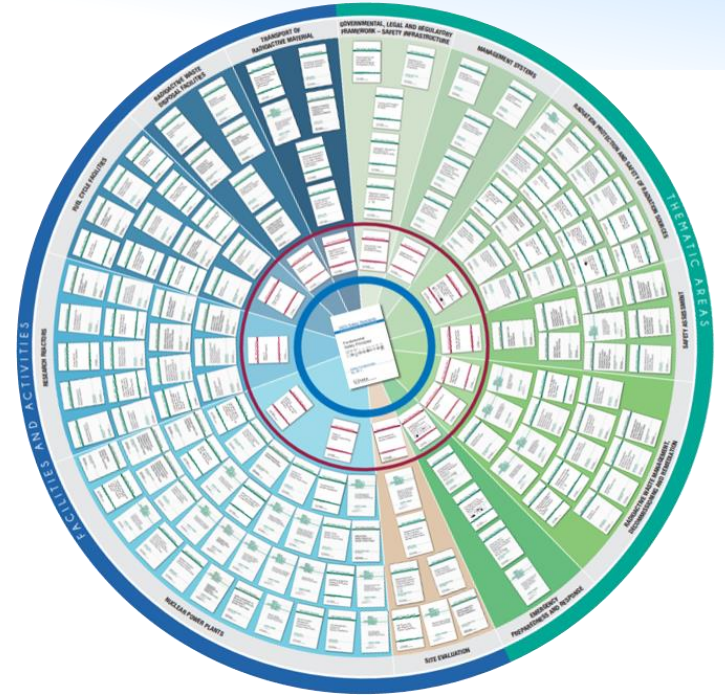
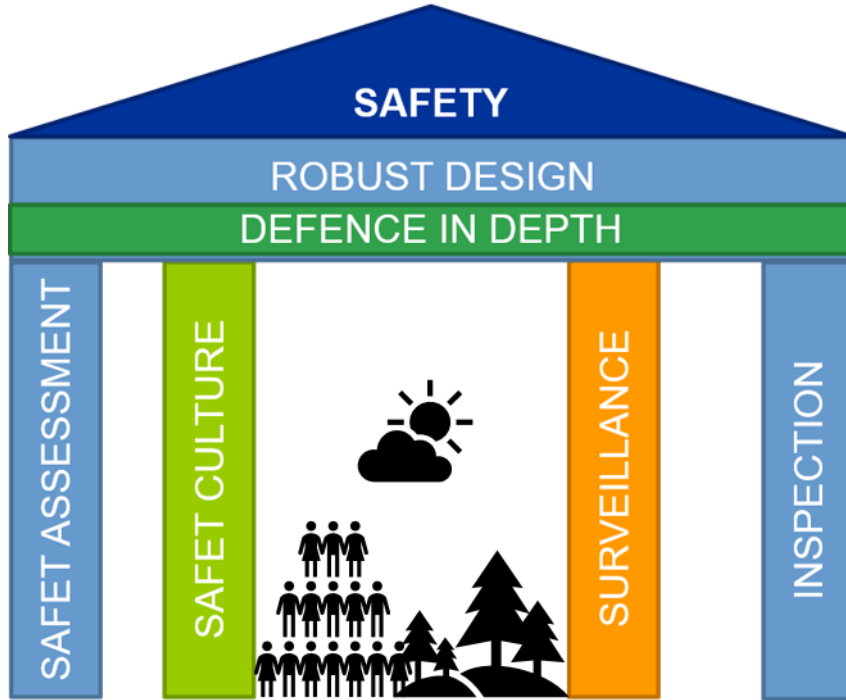
- The achievement of proper operating conditions, prevention of accidents and mitigation of accident consequences, resulting in protection of workers, the public and the environment from undue radiation risks.

**Nuclear safety aims at ensuring control over the process involving radioactive sources, where particularly for NPP shall consider all plant states**

plant states (*considered in design*)

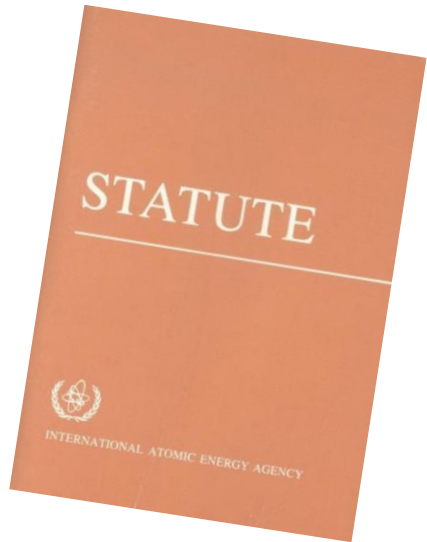


# How nuclear safety could be achieved?



# IAEA Safety Standards

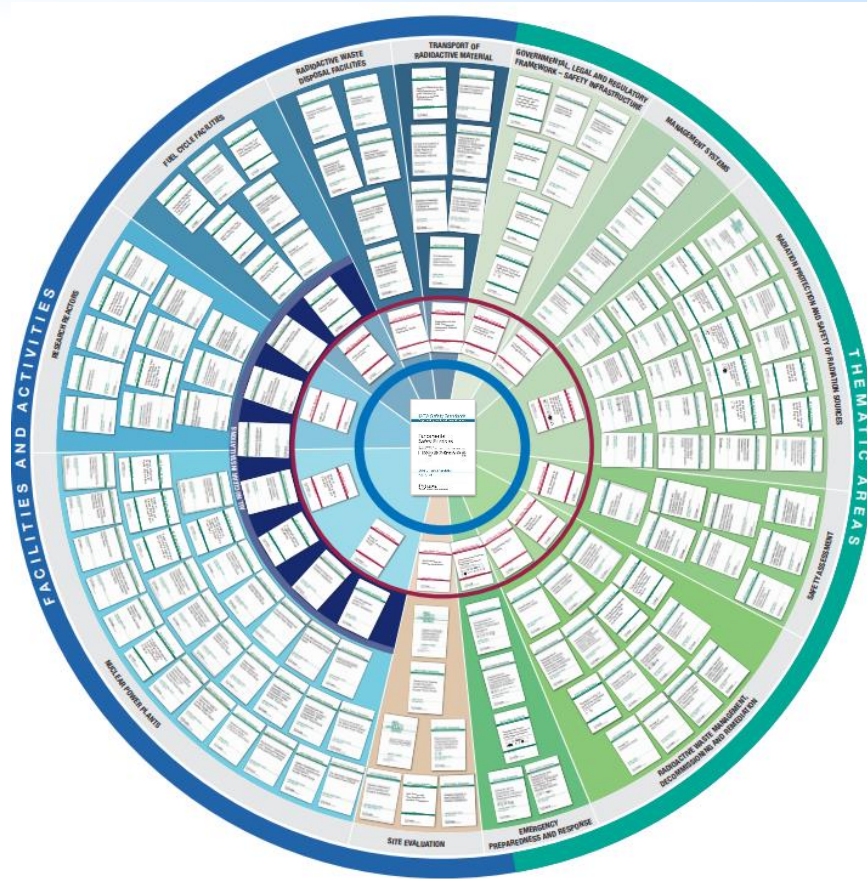
# Safety Standards Hierarchy



Under article III.A.6 of IAEA statute, the IAEA is entitled to:

*“To establish or adopt, in consultation and, where appropriate, in collaboration with the competent organs of the United Nations and with the specialized agencies concerned, standards of safety for protection of health and minimization of danger to life and property...”*

# Safety Standards Hierarchy



# 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



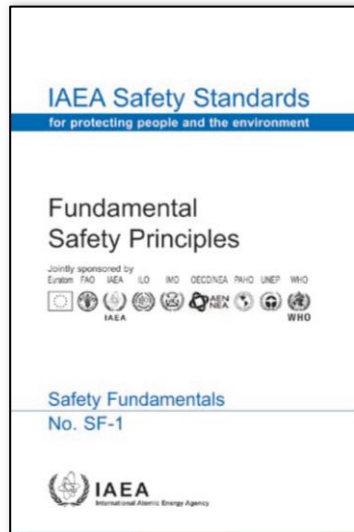
Safety Fundamentals

No. SF-1



# The Fundamental Safety Objective

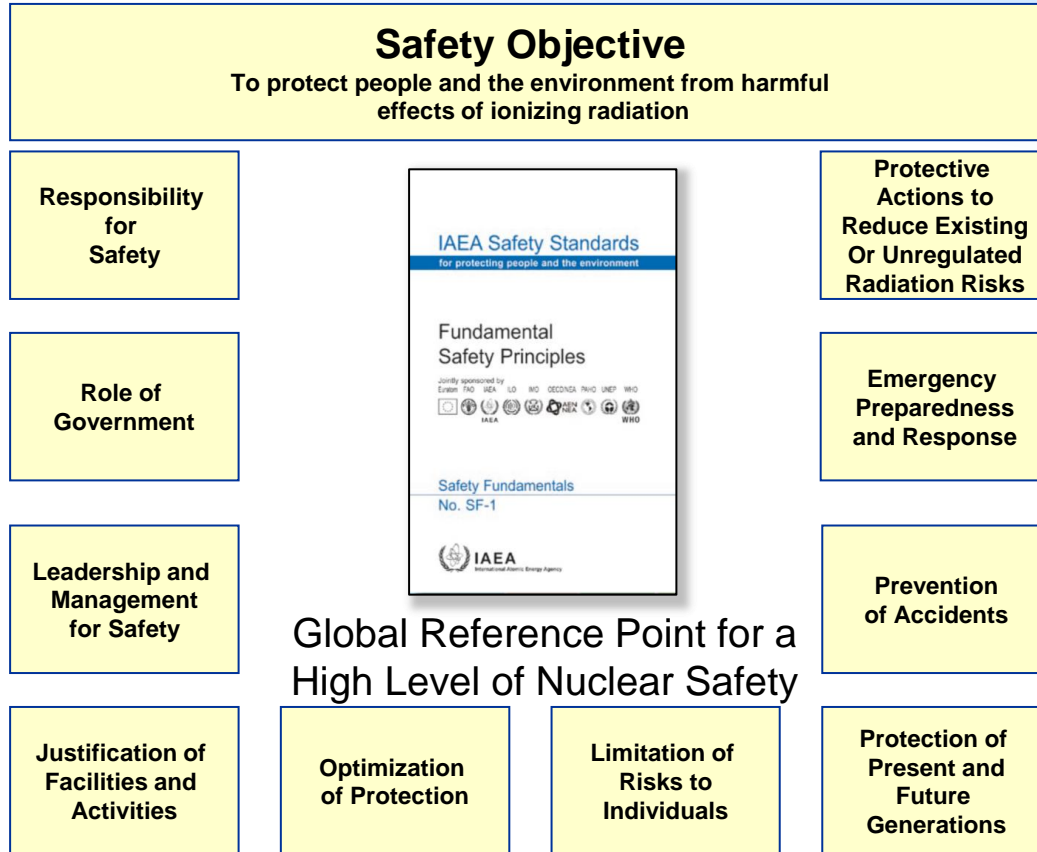
For operation of facilities or for conducting activities that give rise to radiation risks the **fundamental safety objective** is to **protect people and the environment from harmful effects of ionizing radiation**



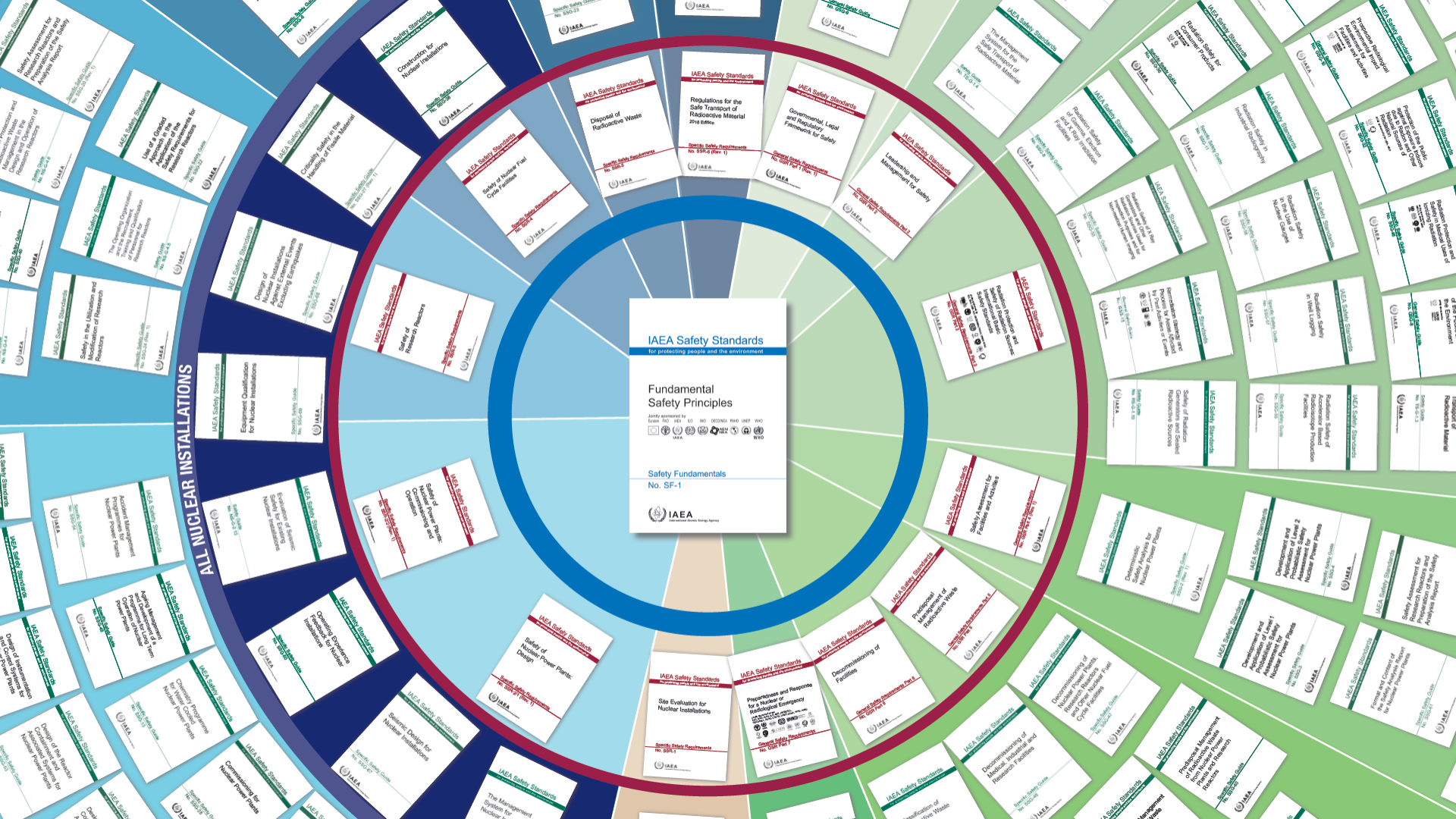
To achieve this, measures have to be taken:

- To control the **radiation exposure** of people and the **release of radioactive material** to the environment;
- To restrict the **likelihood of events** that might lead to a loss of control over a nuclear reactor core, nuclear chain reaction, radioactive source or any other source of radiation;
- To **mitigate the consequences** of such events if they were to occur.

# Safety Standards Hierarchy







ALL NUCLEAR INSTALLATIONS

**IAEA Safety Standards**  
for protecting people and the environment

**Fundamental Safety Principles**

Safety Fundamentals  
No. SF-1

IAEA  
International Atomic Energy Agency

**IAEA Safety Standards**  
Regulations for the Safe Transport of Radioactive Material 2018 edition

**IAEA Safety Standards**  
Governmental, Legal and Regulatory Framework for Safety

**IAEA Safety Standards**  
Licensing and Management for Safety

**IAEA Safety Standards**  
Safety of Production and Industrial Radiography

**IAEA Safety Standards**  
Safety of Radiation Protection

**IAEA Safety Standards**  
Safety of Radiation Protection

**IAEA Safety Standards**  
Safety of Radiation Protection

**IAEA Safety Standards**  
Safety of Nuclear Fuel Cycle Facilities

**IAEA Safety Standards**  
Safety of Research Reactors

**IAEA Safety Standards**  
Design of Accelerator Installations

**IAEA Safety Standards**  
Safety in the Mitigation and Recovery of Accidents

**IAEA Safety Standards**  
Safety of Production and Industrial Radiography

**IAEA Safety Standards**  
Safety of Production and Industrial Radiography

**IAEA Safety Standards**  
Safety of Production and Industrial Radiography

**IAEA Safety Standards**  
Safety of Production and Industrial Radiography

**IAEA Safety Standards**  
Safety of Production and Industrial Radiography

**IAEA Safety Standards**  
Safety of Nuclear Power Plants

**IAEA Safety Standards**  
Site Evaluation for Nuclear Installations

**IAEA Safety Standards**  
Preparation and Response for a Nuclear or Radiological Emergency

**IAEA Safety Standards**  
Decommissioning of Facilities

**IAEA Safety Standards**  
Decommissioning of Medical Installations and Research Facilities

**IAEA Safety Standards**  
Development and Implementation of Safety Management Systems for Nuclear Power Plants

**IAEA Safety Standards**  
Safety Assessment for Rehabilitation and Decommissioning of Research and Test Reactors

**IAEA Safety Standards**  
General Design for Nuclear Installations

**IAEA Safety Standards**  
General Design for Nuclear Installations

**IAEA Safety Standards**  
General Design for Nuclear Installations

**IAEA Safety Standards**  
General Design for Nuclear Installations

**IAEA Safety Standards**  
General Design for Nuclear Installations

**IAEA Safety Standards**  
General Design for Nuclear Installations

**IAEA Safety Standards**  
General Design for Nuclear Installations

**IAEA Safety Standards**  
General Design for Nuclear Installations

**IAEA Safety Standards**  
General Design for Nuclear Installations

**IAEA Safety Standards**  
General Design for Nuclear Installations

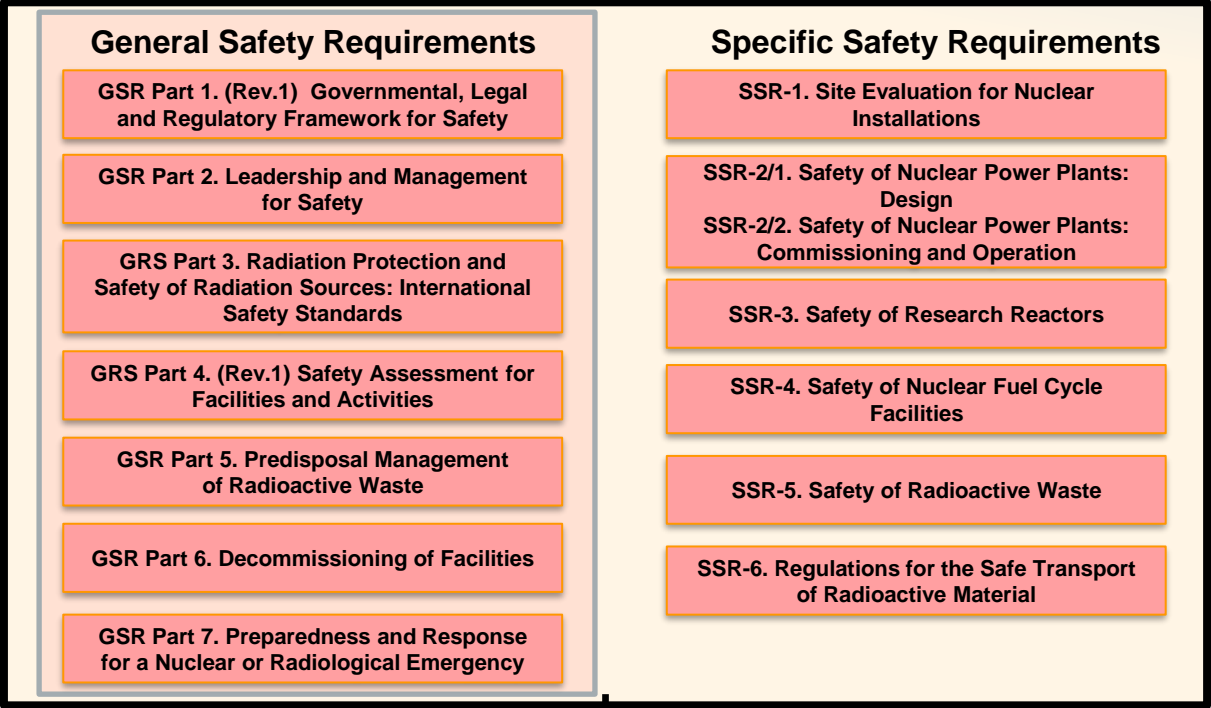
**IAEA Safety Standards**  
General Design for Nuclear Installations

**IAEA Safety Standards**  
General Design for Nuclear Installations

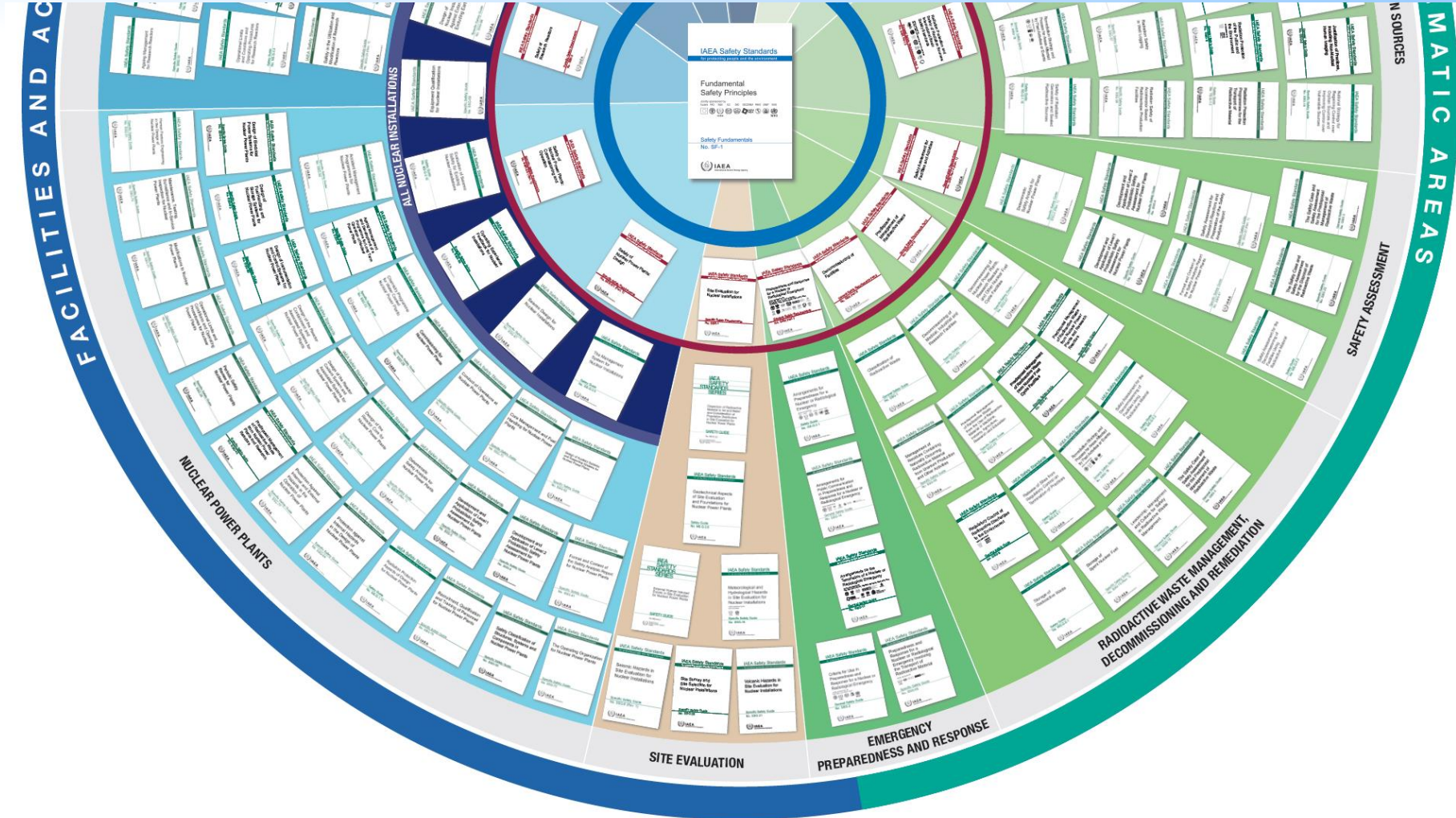
IAEA Safety Standards for protecting people and the environment

# Safety Standards Hierarchy

## Safety Fundamentals SF-1. Fundamental Safety Principles



## Collection of General Safety Guides (GSG) and Specific Safety Guides (SSG)



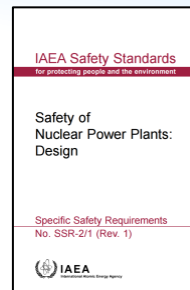
# Design Safety



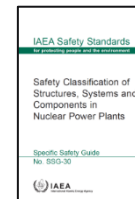
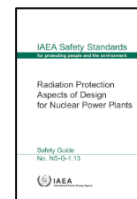
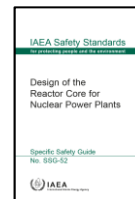
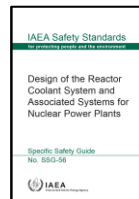
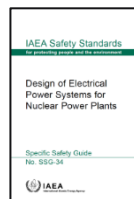
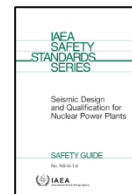
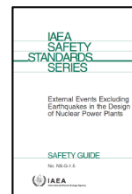
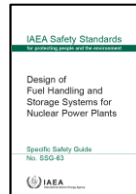
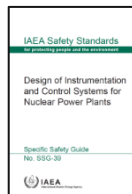
Safety objectives and safety principles



Functional conditions required for safety



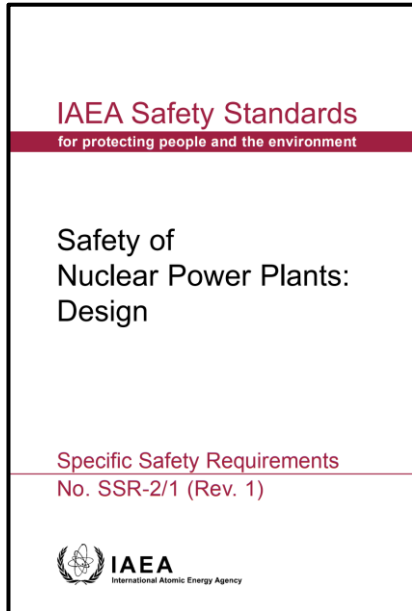
Guidance on how to fulfil the requirements



# Design safety

## Introduction to IAEA Specific Safety Requirements SSR-2/1 (Rev. 1)

# SSR 2/1 (Rev. 1): Safety of Nuclear Power Plants: Design



Published in 2016, revised to consider the main observations and lessons from the accident at the Fukushima Daiichi Nuclear Power Plant. The review revealed no significant areas of weakness and resulted in a small set of amendments to strengthen the requirements and facilitate their implementation.

Requirements applicable to the NPP design and elaborates on the safety objective, safety principles and concepts that provide the basis for deriving the safety requirements that must be met for the NPP design.

- Useful for organizations involved in design, manufacture, construction, modification, maintenance, operation and decommissioning of NPP, as well as for regulatory bodies

# Importance of SSR for NPP Design (1/2)

Define safety approach and establish safety “level” for NPP designs

- reflects the state of the art
- reflects the views and the licensing practices of the majority of IAEA Member States
- based on large consensus

Provide links with requirements for site evaluation and for operation

- taking into consideration impact of site on design
- ensuring safe operation and maintenance of plant

# Importance of SSR for NPP Design (2/2)

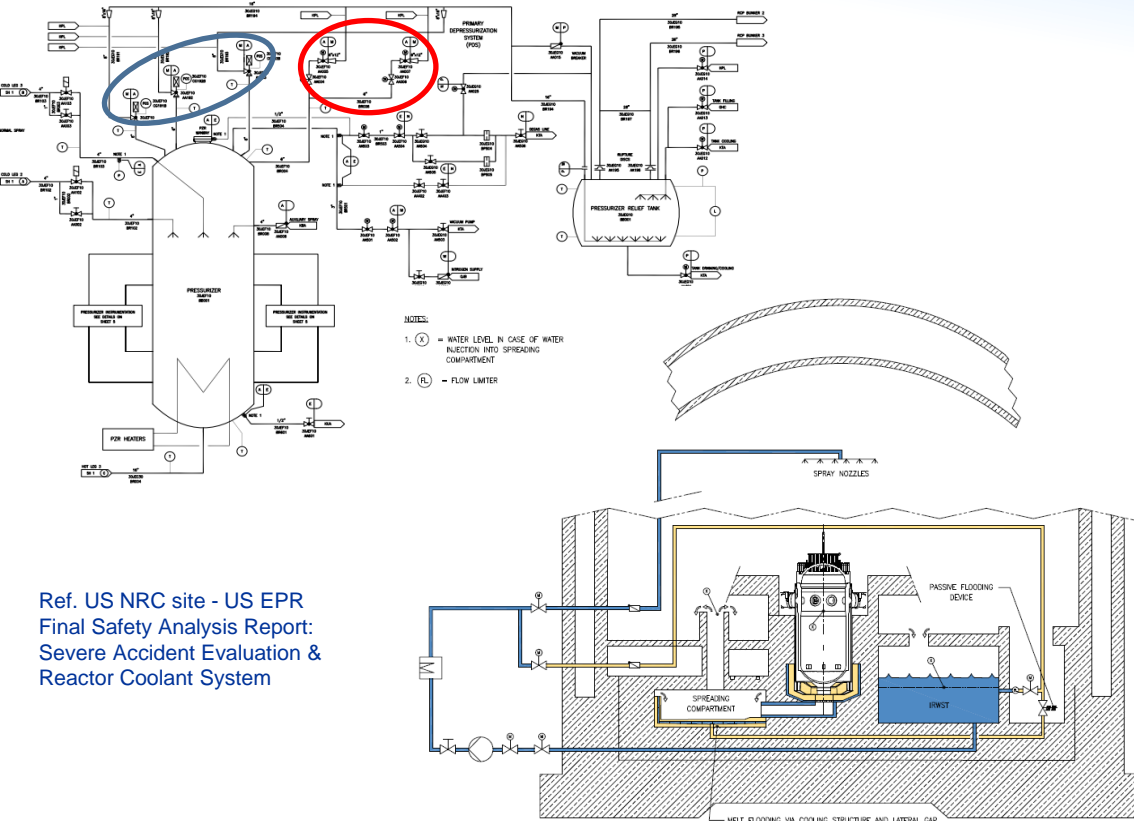
Requirements collected in this safety standard

- 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



# SSR 2/1 (Rev. 1): Safety of Nuclear Power Plants: Design (1/5)

Reinforce the application of the Defence-in-Depth concept, by implementing independent Defence-in-Depth provisions, mainly between provisions required for levels 3 and 4



Ref. US NRC site - US EPR Final Safety Analysis Report: Severe Accident Evaluation and Reactor Coolant System

# SSR 2/1 (Rev. 1): Safety of Nuclear Power Plants: Design (2/5)



Construction 18m embankment to protect against tsunami Hamaoka NPP, Japan

Stressing the need for sufficient and adequate margins to avoid cliff edge effects. For items that ultimately prevent large or early releases, margins are required also for hazards more severe than those selected for the design basis

# SSR 2/1 (Rev. 1): Safety of Nuclear Power Plants: Design (3/5)



Wolsong NPP, Republic of Korea

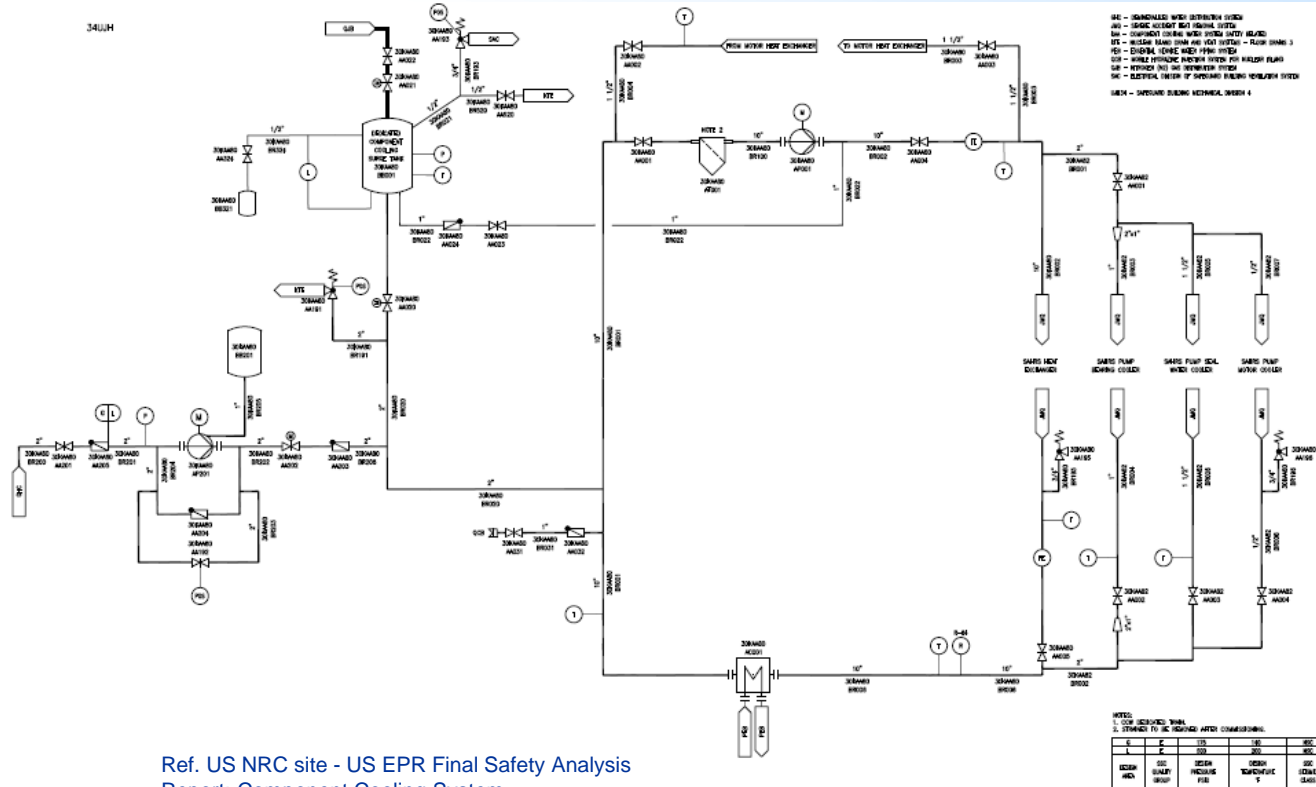
Multi-unit site considerations related to the independence of dedicated, to each unit, safety systems for DBA and additional safety features for DEC.

DBA=Design Basis Accidents

DEC=Design Extension Conditions

# SSR 2/1 (Rev. 1): Safety of Nuclear Power Plants: Design (4/5)

- Reinforced capabilities for heat transfer to the UHS. Alternative heat sink or different access is required if heat transfer cannot be ensured in conditions generated by hazards more severe than those selected for the design basis



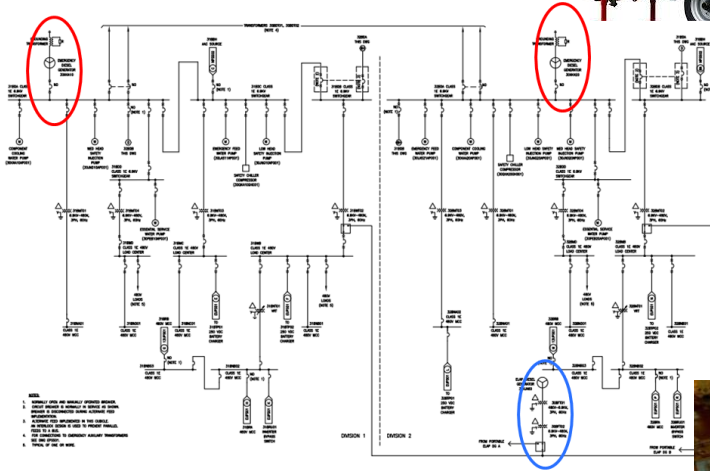
UHS=Ultimate Heat Sink

Ref. US NRC site - US EPR Final Safety Analysis Report: Component Cooling System

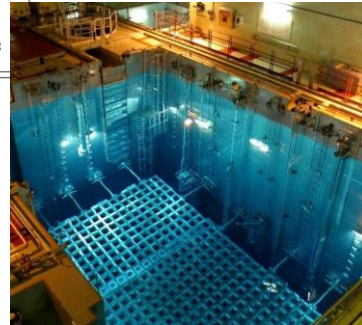
# SSR 2/1 (Rev. 1): Safety of Nuclear Power Plants: Design (5/5)



- Implementation of features (design, procedures, etc.) to enable the use of non permanent equipment
- Reinforced capabilities for power supply in DECUs
- Additional measures for spent fuel pool instrumentation, cooling and maintaining inventory



Ref. US NRC site - US EPR Final Safety Analysis Report: Electrical power distribution




# SSR 2/1 (Rev. 1) : Table of contents (1/2)

**IAEA Safety Standards**  
for protecting people and the environment

**Safety of Nuclear Power Plants: Design**

Specific Safety Requirements  
No. SSR-2/1 (Rev. 1)



CONTENTS	
1. INTRODUCTION .....	1
Background (1.1–1.3) .....	1
Objective (1.4–1.5) .....	2
Scope (1.6–1.8) .....	2
Structure (1.9) .....	3
2. APPLYING THE SAFETY PRINCIPLES AND CONCEPTS (2.1–2.5) .....	3
Radiation protection in design (2.6–2.7) .....	4
Safety in design (2.8–2.11) .....	5
The concept of defence in depth (2.12–2.14) .....	6
Maintaining the integrity of design of the plant throughout the lifetime of the plant (2.15–2.18) .....	9
3. MANAGEMENT OF SAFETY IN DESIGN .....	10
Requirement 1: Responsibilities in the management of safety in plant design (3.1) .....	10
Requirement 2: Management system for plant design (3.2–3.4) .....	10
Requirement 3: Safety of the plant design throughout the lifetime of the plant (3.5–3.6) .....	11
4. PRINCIPAL TECHNICAL REQUIREMENTS .....	12
Requirement 4: Fundamental safety functions (4.1–4.2) .....	12
Requirement 5: Radiation protection in design (4.3–4.4) .....	13
Requirement 6: Design for a nuclear power plant (4.5–4.8) .....	13
Requirement 7: Application of defence in depth (4.9–4.13A) .....	14
Requirement 8: Interfaces of safety with security and safeguards .....	16
Requirement 9: Proven engineering practices (4.14–4.16) .....	16
Requirement 10: Safety assessment (4.17–4.18) .....	17
Requirement 11: Provision for construction (4.19) .....	17
Requirement 12: Features to facilitate radioactive waste management and decommissioning (4.20) .....	17


GENERAL PLANT DESIGN .....	18
Design basis .....	18
Requirement 13: Categories of plant states (5.1–5.2) .....	18
Requirement 14: Design basis for items important to safety (5.3) .....	19
Requirement 15: Design limits (5.4) .....	19
Requirement 16: Postulated initiating events (5.5–5.15) .....	19
Requirement 17: Internal and external hazards (5.15A–5.22) .....	21
Requirement 18: Engineering design rules (5.23) .....	23
Requirement 19: Design basis accidents (5.24–5.26) .....	23
Requirement 20: Design extension conditions (5.27–5.32) .....	24
Requirement 21: Physical separation and independence of safety systems (5.33) .....	26
Requirement 22: Safety classification (5.34–5.36) .....	26
Requirement 23: Reliability of items important to safety (5.37–5.38) .....	27
Requirement 24: Common cause failures .....	27
Requirement 25: Single failure criterion (5.39–5.40) .....	27
Requirement 26: Fail-safe design (5.41) .....	28
Requirement 27: Support service systems (5.42–5.43) .....	28
Requirement 28: Operational limits and conditions for safe operation (5.44) .....	28
Design for safe operation over the lifetime of the plant .....	29
Requirement 29: Calibration, testing, maintenance, repair, replacement, inspection and monitoring of items important to safety (5.45–5.47) .....	29
Requirement 30: Qualification of items important to safety (5.48–5.50) .....	30
Requirement 31: Ageing management (5.51–5.52) .....	30
Human factors .....	31
Requirement 32: Design for optimal operator performance (5.53–5.62) .....	31
Other design considerations .....	33
Requirement 33: Safety systems, and safety features for design extension conditions, of units of a multiple unit nuclear power plant (5.63) .....	33
Requirement 34: Systems containing fissile material or radioactive material .....	33
Requirement 35: Nuclear power plants used for cogeneration of heat and power, heat generation or desalination .....	33

# SSR 2/1 (Rev. 1) : Table of contents (2/2)

**IAEA Safety Standards**  
for protecting people and the environment

**Safety of Nuclear Power Plants: Design**

Specific Safety Requirements  
No. SSR-2/1 (Rev. 1)



Requirement 36: Escape routes from the plant (5.64–5.65) . . . . .	33	Requirement 59: Provision of instrumentation (6.31) . . . . .	46
Requirement 37: Communication systems at the plant (5.66–5.67) . . . . .	34	Requirement 60: Control systems . . . . .	46
Requirement 38: Control of access to the plant (5.68) . . . . .	34	Requirement 61: Protection system (6.32–6.33) . . . . .	46
Requirement 39: Prevention of unauthorized access to, or interference with, items important to safety. . . . .	34	Requirement 62: Reliability and testability of instrumentation and control systems (6.34–6.36) . . . . .	47
Requirement 40: Prevention of harmful interactions of systems important to safety (5.69–5.70) . . . . .	35	Requirement 63: Use of computer based equipment in systems important to safety (6.37) . . . . .	48
Requirement 41: Interactions between the electrical power grid and the plant . . . . .	35	Requirement 64: Separation of protection systems and control systems (6.38) . . . . .	48
Safety analysis . . . . .	35	Requirement 65: Control room (6.39–6.40A) . . . . .	49
Requirement 42: Safety analysis of the plant design (5.71–5.76) . . . . .	35	Requirement 66: Supplementary control room (6.41) . . . . .	49
<b>DESIGN OF SPECIFIC PLANT SYSTEMS. . . . .</b>	<b>37</b>	Requirement 67: Emergency response facilities on the site (6.42) . . . . .	50
Reactor core and associated features . . . . .	37	Emergency power supply . . . . .	50
Requirement 43: Performance of fuel elements and assemblies (6.1–6.3) . . . . .	37	Requirement 68: Design for withstanding the loss of off-site power (6.43–6.45A) . . . . .	50
Requirement 44: Structural capability of the reactor core . . . . .	38	Supporting systems and auxiliary systems . . . . .	52
Requirement 45: Control of the reactor core (6.4–6.6) . . . . .	38	Requirement 69: Performance of supporting systems and auxiliary systems . . . . .	52
Requirement 46: Reactor shutdown (6.7–6.12) . . . . .	39	Requirement 70: Heat transport systems (6.46) . . . . .	52
Reactor coolant systems . . . . .	40	Requirement 71: Process sampling systems and post-accident sampling systems (6.47) . . . . .	52
Requirement 47: Design of reactor coolant systems (6.13–6.16) . . . . .	40	Requirement 72: Compressed air systems . . . . .	52
Requirement 48: Overpressure protection of the reactor coolant pressure boundary . . . . .	41	Requirement 73: Air conditioning systems and ventilation systems (6.48–6.49) . . . . .	53
Requirement 49: Inventory of reactor coolant . . . . .	41	Requirement 74: Fire protection systems (6.50–6.54) . . . . .	53
Requirement 50: Cleanup of reactor coolant (6.17) . . . . .	41	Requirement 75: Lighting systems . . . . .	54
Requirement 51: Removal of residual heat from the reactor core . . . . .	41	Requirement 76: Overhead lifting equipment (6.55) . . . . .	54
Requirement 52: Emergency cooling of the reactor core (6.18–6.19) . . . . .	42	Other power conversion systems . . . . .	55
Requirement 53: Heat transfer to an ultimate heat sink (6.19A–6.19B) . . . . .	42	Requirement 77: Steam supply system, feedwater system and turbine generators (6.56–6.58) . . . . .	55
Containment structure and containment system . . . . .	43	Treatment of radioactive effluents and radioactive waste . . . . .	55
Requirement 54: Containment system for the reactor . . . . .	43	Requirement 78: Systems for treatment and control of waste (6.59–6.60) . . . . .	55
Requirement 55: Control of radioactive releases from the containment (6.20–6.21) . . . . .	43	Requirement 79: Systems for treatment and control of effluents (6.61–6.63) . . . . .	56
Requirement 56: Isolation of the containment (6.22–6.24) . . . . .	43	Fuel handling and storage systems . . . . .	56
Requirement 57: Access to the containment (6.25–6.26) . . . . .	44	Requirement 80: Fuel handling and storage systems (6.64–6.68A) . . . . .	56
Requirement 58: Control of containment conditions (6.27–6.30) . . . . .	45	Radiation protection . . . . .	59
Instrumentation and control systems . . . . .	46	Requirement 81: Design for radiation protection (6.69–6.76) . . . . .	59
		Requirement 82: Means of radiation monitoring (6.77–6.84) . . . . .	60

# Safety approach for the design of NPPs

Safety  
Objective

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

Principles

**P5. Optimization of Protection**

**P6. Limitation of Risks to Individuals**

**P7. Protection of Present and Future Generations**

**P8. Prevention of Accidents**

prerequisites

**P9. Emergency Preparedness and Response**



# Foundations of NPP Safety

## Fundamental Safety Principles

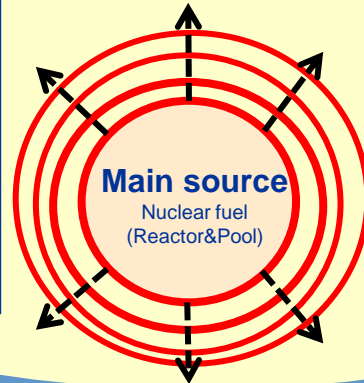
**Safety Objective:** Protect people and the environment from harmful effects of radiation

- 10 Safety principles:

- No. 5 – Optimization of protection
- No. 6 – Limitation of risks to individuals
- No. 7 – Protection of present and future generations
- No. 8 – Prevention and mitigation of accidents
- No. 9 – Emergency preparedness and response

## Defence in depth & PE

- Based on a number of consecutive and independent levels of protection including physical barriers
- Practical elimination of plant event Sequences that would lead to an early radioactive release or a large radioactive release



## Fundamental Safety Functions

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

Ensure protection of barriers

The current implementation of DiD at LWRs comprises 5 levels of protection and 4 physical barriers (fuel matrix, fuel cladding, reactor coolant boundary and containment building)

# Design safety

## Principal Technical 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

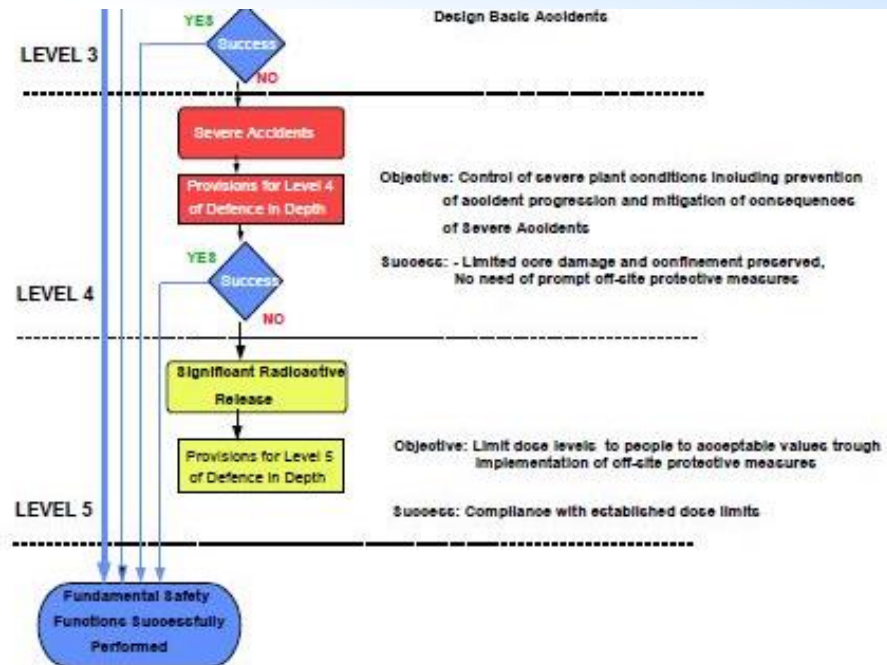
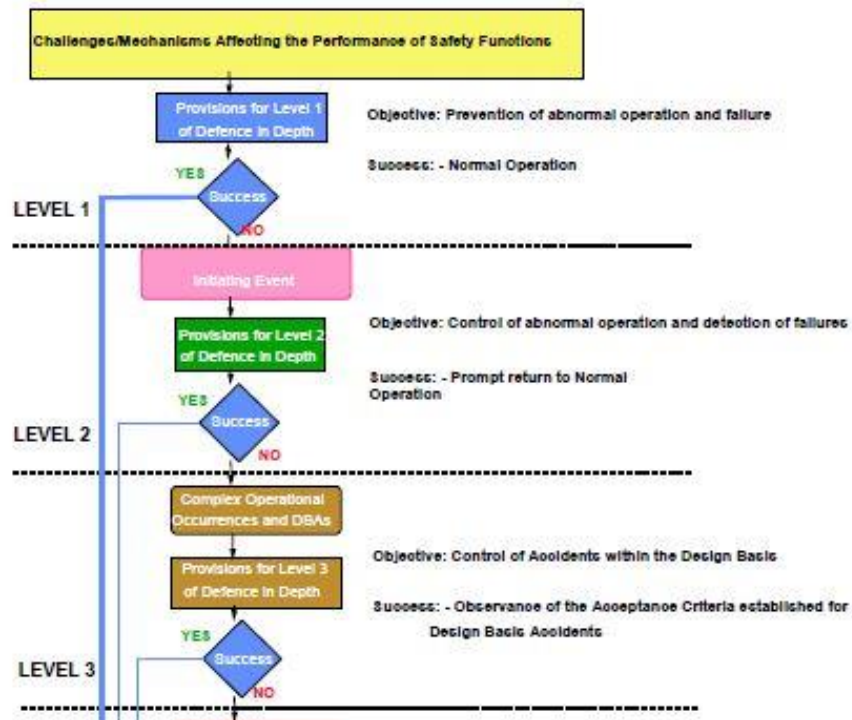
# Principal Technical Requirements

## 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

# Defence in Depth objectives



Ref. IAEA SRS 46 - Assessment of Defence in Depth for Nuclear Power Plants

## **Prevention of deviations from normal operation and the failure of items important to safety**

- Conservatism in siting, design, construction, maintenance and operation.
- Proven engineering practices. Selection of appropriate design codes and materials
- Quality controls, testing, inspection
- Design options that reduce the potential for internal hazards and facilitate operation and maintenance
- Stable control systems
- Consideration of operating experience
- Etc.

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

**Detection and control of deviations from normal operational states in order to prevent anticipated operational occurrences at the plant from escalating to accident conditions**

- Recognition of the fact that postulated initiating events are likely to occur over the operating lifetime despite the care taken to prevent them.
- Provision of specific systems and features in the design and 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.
- The “practical elimination” concept applies to plant event sequences that lead to large or early radioactive releases.

# 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.

# Design safety

## General Plant Design Requirements

# General Plant Design

- Design Basis
  - Plant States
  - Design basis of items important to safety
  - Postulated Initiating events
  - Internal and external hazards
  - Design rules
  - Design Basis Accident
  - 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.

- 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

# Concepts

## **Anticipated operational occurrence (AOO).**

An operational process deviating from normal operation which is expected to occur at least once during the operating lifetime of a facility but which, in view of appropriate design provisions, does not cause any significant damage to items important to safety or lead to accident conditions.

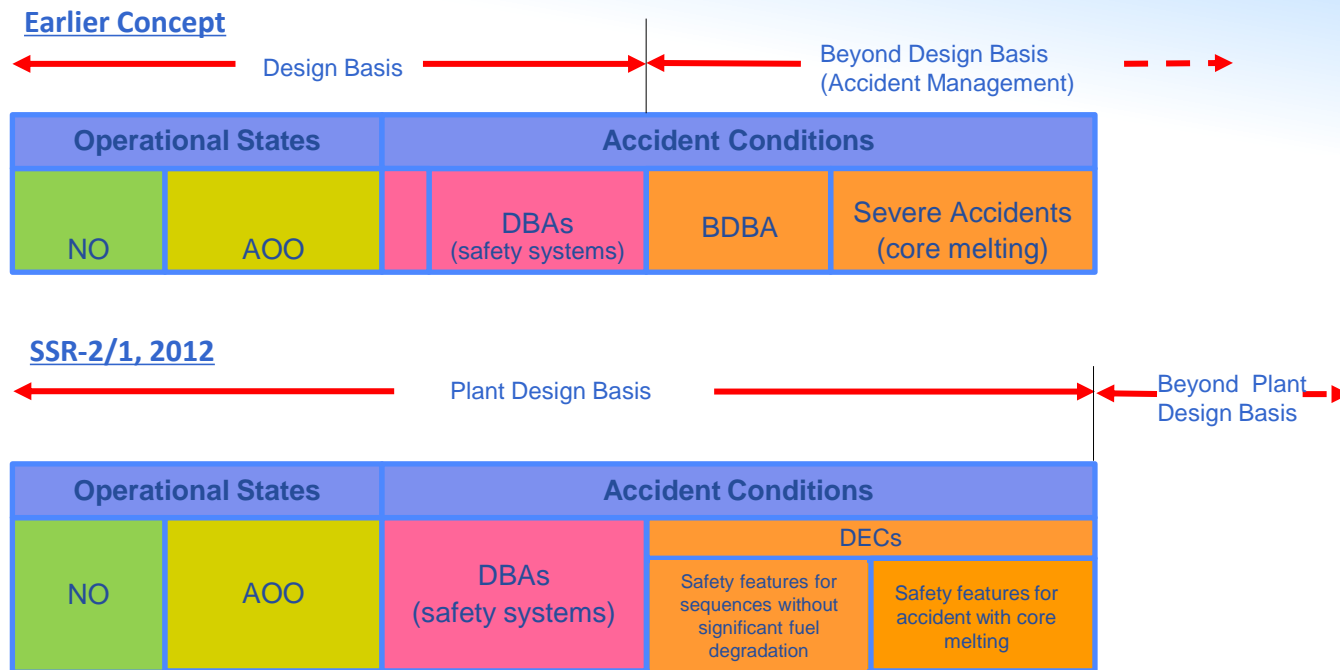
## **Design basis accident (DBA)**

Accident conditions against which a facility is designed according to established design criteria, and for which the damage to the fuel and the release of radioactive material are kept within authorized limits.

## **Design Extension Conditions (DECs). IAEA Definition:**

Postulated accident conditions that are not considered for design basis accidents, but that are considered in the design process of the facility in accordance with best estimate methodology, and for which releases of radioactive material are kept within acceptable limits. Design extension conditions could include conditions in events without significant fuel degradation and conditions with core melting.

# Plant States



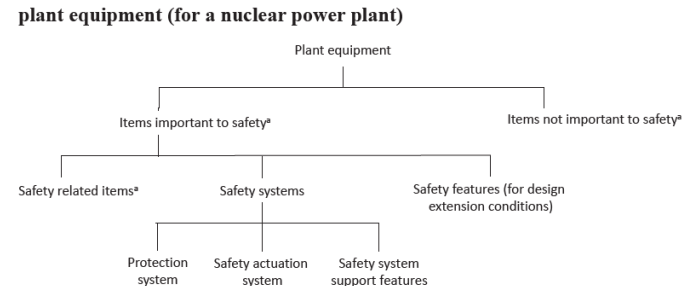
## Design basis (IAEA Safety Glossary, Edition 2022)

The range of conditions and *events* taken explicitly into account in the *design* of *structures, systems and components* and equipment of a *facility*, according to established criteria, such that the *facility* can withstand them without exceeding *authorized limits*.

## 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.



<sup>a</sup> In this context, an 'item' is a structure, system or component.



## 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

# 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.

# Design Extension Conditions (DECs)

IAEA Design Safety Requirements: to derive the set of DECs systematically on the basis of

- Engineering judgement
- Deterministic evaluations (DSA)
- Probabilistic considerations (PSA)
- Operating experience, particularly LWR technology

DECs are technology dependent

Recommended DECs (except for SBO) are not available in IAEA Safety Standards

# DECs without Fuel Degradation (1/3)

Exemplary listing some countries also refer to as deterministically identified, may include

- anticipated transient without scram (ATWS)
- station blackout (SBO)
- loss of core cooling in the residual heat removal mode
- extended loss of cooling of fuel pool and inventory
- loss of normal access to the ultimate heat sink

# DECs without Fuel Degradation (2/3)

## DECs derived from PSA might include (examples)

- total loss of feed water
- LOCA plus loss of one emergency core cooling system (high pressure or the low pressure emergency cooling system)
- loss of the component cooling water system or the essential service water system
- uncontrolled boron dilution
- multiple steam generator tube ruptures (for PWRs)
- steam generator tube ruptures induced by main steam line break (for PWRs)
- uncontrolled level drop during mid-loop operation (for PWRs) or during refueling

# DECs without Fuel Degradation (3/3)

All these cases are only DEC when the plant is designed for them.

Otherwise they are beyond design basis accidents

# DECs with Core Melting

Necessary to identify a representative group of severe accident conditions to be used for defining the design basis of the mitigatory safety features

Important: sufficient knowledge on different severe accident phenomena

Main objective: cooling and stabilization of the molten fuel and the removal of heat from the containment

Present knowledge on physical and chemical phenomena: sound base for design basis

# Use of Non Permanent Equipment

- After the Fukushima accident the revision of SSR 2/1 requires design provisions to enable the connection of some types of non permanent equipment in a smooth and safe manner (for situations exceeding the design basis).
- For new plants, the features for hooking up non permanent equipment should not be necessary for DBA and DEC.



# Fundamental safety objective – DiD and PE

Protect people and the environment from harmful effects of ionizing radiation

Implement Defence in Depth concept to prevent accidents and to mitigate the consequences within acceptable limits should accident occur

Practical elimination of plant event sequences that would lead to an early radioactive release or a large radioactive release

# Practical Elimination

## Formulations on practical elimination in SSR-2/1 (Rev. 1):

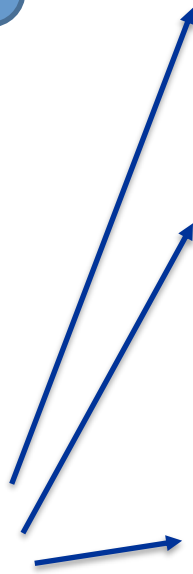
Made in terms of objectives of:

- Radiation protection (4.3)
- Level 4 of DiD (2.13)
- Margins against external hazards (5.21A) / DEC for core melt (5.27, 5.31)
- Safety Analysis – margins and prevention of CE effects (5.73)
- Containment design (6.28A)
- SFP design (6.68)

# Practical elimination: Safety Standards

## SSR-2/1 (Rev. 1), Par 2.13 (4)

*“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 are required to be ‘practically eliminated’ ”*

- 
- Radioactive release for which off-site protective actions would be **necessary** but would be **unlikely** to be **fully effective** in due time
  - 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
  - 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



## 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.

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**', and that there would be no, or only minor, potential radiological consequences for plant states with a significant likelihood of occurrence.

4.4 Acceptable limits for radiation protection associated with the relevant categories of plant states shall be established, consistent with the regulatory requirements.

# Practical Elimination

## Requirement 20: Design extension conditions (DECs)

...

**5.31 The design shall be such that the possibility of plant states arising that could lead to early or to large releases is ‘practically eliminated’. \***

**5.31A The design shall be such that for design extension conditions, protective actions that are limited in terms of lengths of time 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.**

# Practical Elimination

## Requirement 58: Control of containment conditions

...

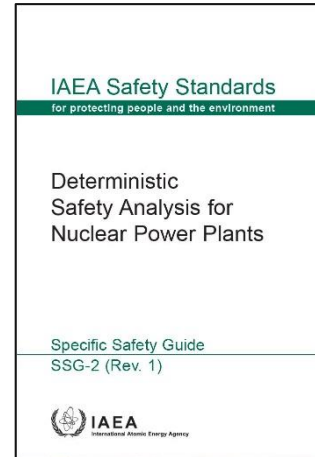
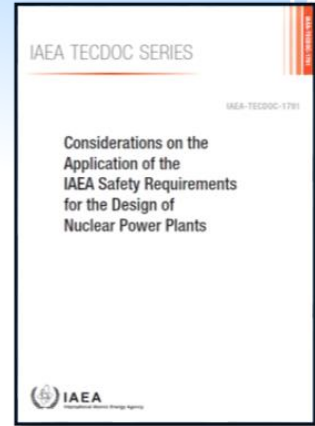
**6.28A Design provision shall be made to prevent the loss of the structural integrity of the containment in all plant states. The use of this provision shall not lead to an early radioactive release or a large radioactive release.**

# Plant event sequences to be considered for Practical Elimination



IAEA

- 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
- Severe accident sequences that could lead to early containment failure
  - Highly energetic direct containment heating
  - Large steam explosion
  - Explosion of combustible gases, including hydrogen and carbon monoxide
- Severe accident sequences that could lead to late containment failure
  - Basemat penetration or containment bypass during MCCI
  - Long term loss of containment heat removal
  - Explosion of combustible gases, including hydrogen and carbon monoxide
- Severe accident with containment by pass
  - LOCA with the potential to drive the leakage outside of the containment,
  - Induced SGTR or severe accident in which the containment is open (shutdown mode)
- Significant fuel degradation in storage fuel pool, uncontrolled releases



# Approach to the Justification of Practical Elimination



Definition gives 2 options for demonstration:

- physically impossible
- Extremely unlikely to arise with a high level of confidence

1. Impossibility: Deterministic. Equivalent to probability 0 or reliance on inherent physical characteristics

- Not possible due to physical laws or to physical laws validated within a given range (as long as the boundary conditions are not violated) (e.g. negative coefficient feedbacks, no hydrogen production, absence of water, etc.)
- Indisputable statement that the hazard load is significantly lower than the minimum resistance of the SSC

Application is however limited

No or very low uncertainty



# Approach to the Justification of Practical Elimination



2. High confidence that it is very unlikely:

– Scientific understanding: Probabilistic concept

• Very unlikely = very low probability (avoiding differences between probability and likelihood)

• High confidence: Use of a confidence interval around the mean value or other ways to characterize uncertainty (e.g. mean and standard deviation, variance, percentiles, etc.) for giving sufficient assurances that the probability is indeed very low

– Demonstration should primarily be based on deterministic requirements, and whenever possible, complementary probabilistic analyses should be performed to confirm the extreme unlikelihood of situations.

# Approach to the Justification of Practical Elimination



- A “high level of confidence” (or Possibilities for violating assumptions of a very low probability) should rely on:
  - credible R&D results, tests and experiments
  - Robustness of implemented design features complemented as needed by consideration of operational means
  - Reliable design /manufacturing provisions;
- Engineering judgement
  - The estimate of the probability of every condition should be such that their cumulative contribution do not exceed the target for large or early release frequency established by the regulatory body.
  - The demonstration cannot be achieved alone by showing the compliance with a probabilistic target.
  - Meeting a probabilistic target should not be considered as a justification for not implementing reasonable design or operational measures
  - Combined use o DSA & PSA with due consideration of uncertainties and limitations of the analysis techniques.

# Approach to the Justification of Practical Elimination



- Uncertainties should be reliably determined (models, data, acceptance criteria\*, performances, initial conditions, phenomena, etc.)
- Sensitive analyses should be performed to identify key parameters.
- Acceptance criteria should be met taking into account uncertainties

\* Acceptance criteria usually are defined so that the limit is not exceeded with some margin

# Approach to the Justification of Practical Elimination



- Identification of conditions to be practically eliminated
- Identification of design and other safety provisions for them
- Justification:
  - When feasible based on physical impossibility (e.g. insufficient hydrogen/oxygen concentration, intrinsic reactivity coefficients, etc.)
  - Justification needs to rely primarily on design features complemented as needed by operational means to prevent the conditions
  - Justification based on the robustness of measures implemented to prevent the condition
  - Combined use DSA & PSA (not limited to Boolean models) with consideration of uncertainties with due consideration to the limitations of the analysis techniques.
  - Justification cannot be achieved alone by showing the compliance with a probabilistic value. This should not be considered as an argument for not implementing reasonable design or operational measures
  - The arguments and methods for justification are highly case specific. Demonstrations can be very challenging

# DSA in support of Practical Elimination



Include **deterministic considerations** and **engineering aspects** supplemented by probabilistic considerations, considering **uncertainties** due to limited knowledge of physical phenomena

## Steps

- a) **Identification** of conditions potentially endangering integrity of containment or allow its bypassing
- b) Implementation of **design** and operational provisions to 'practically eliminate' their possibility, including margins to cope with uncertainties
- c) Final **confirmation of adequacy** of provisions by DSA, complemented by PSA and engineering judgement

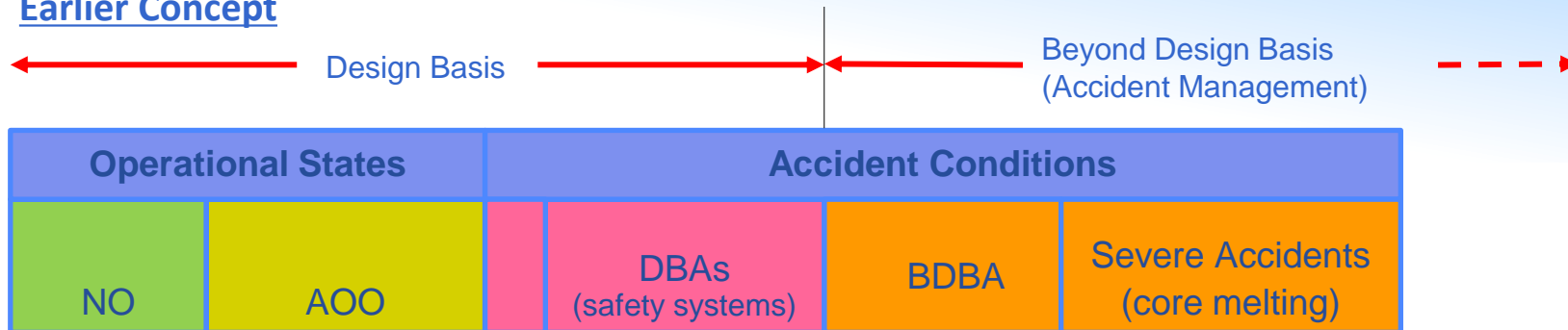
Demonstration not based solely on low probability values

- **deterministic definition** and base on **performance of safety features** making event sequences extremely unlikely

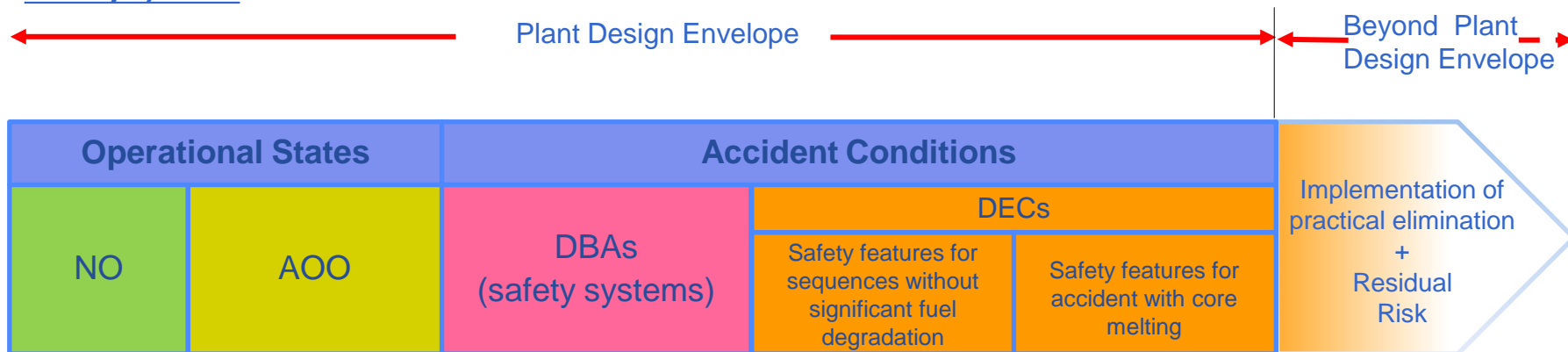
Claim that conditions potentially resulting in early/large radioactive release are **physically impossible**: examine **system inherent safety characteristics** to demonstrate that they cannot , by the laws of nature, occur and that fundamental safety will be achieved

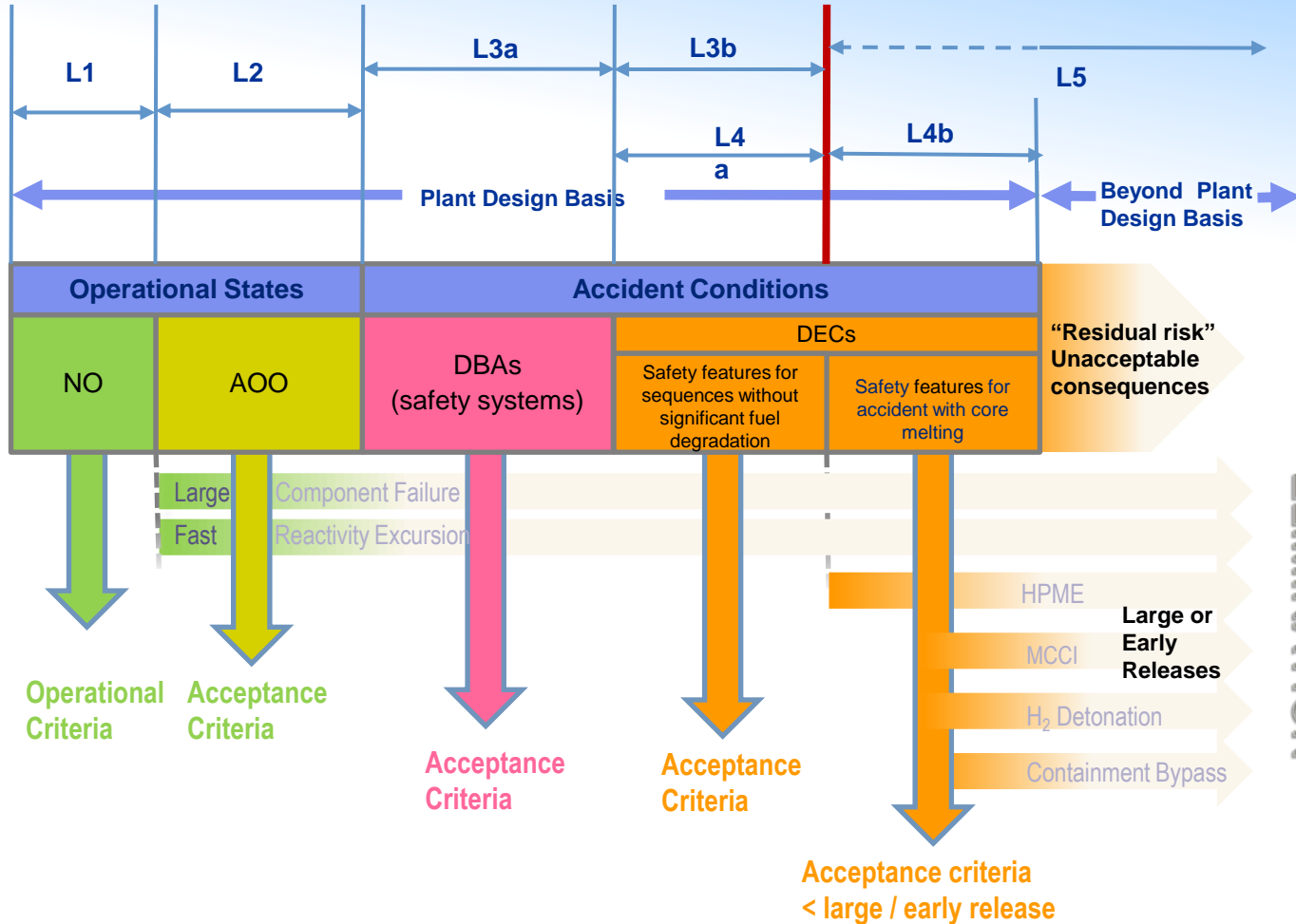
# Practical Elimination & Plant States

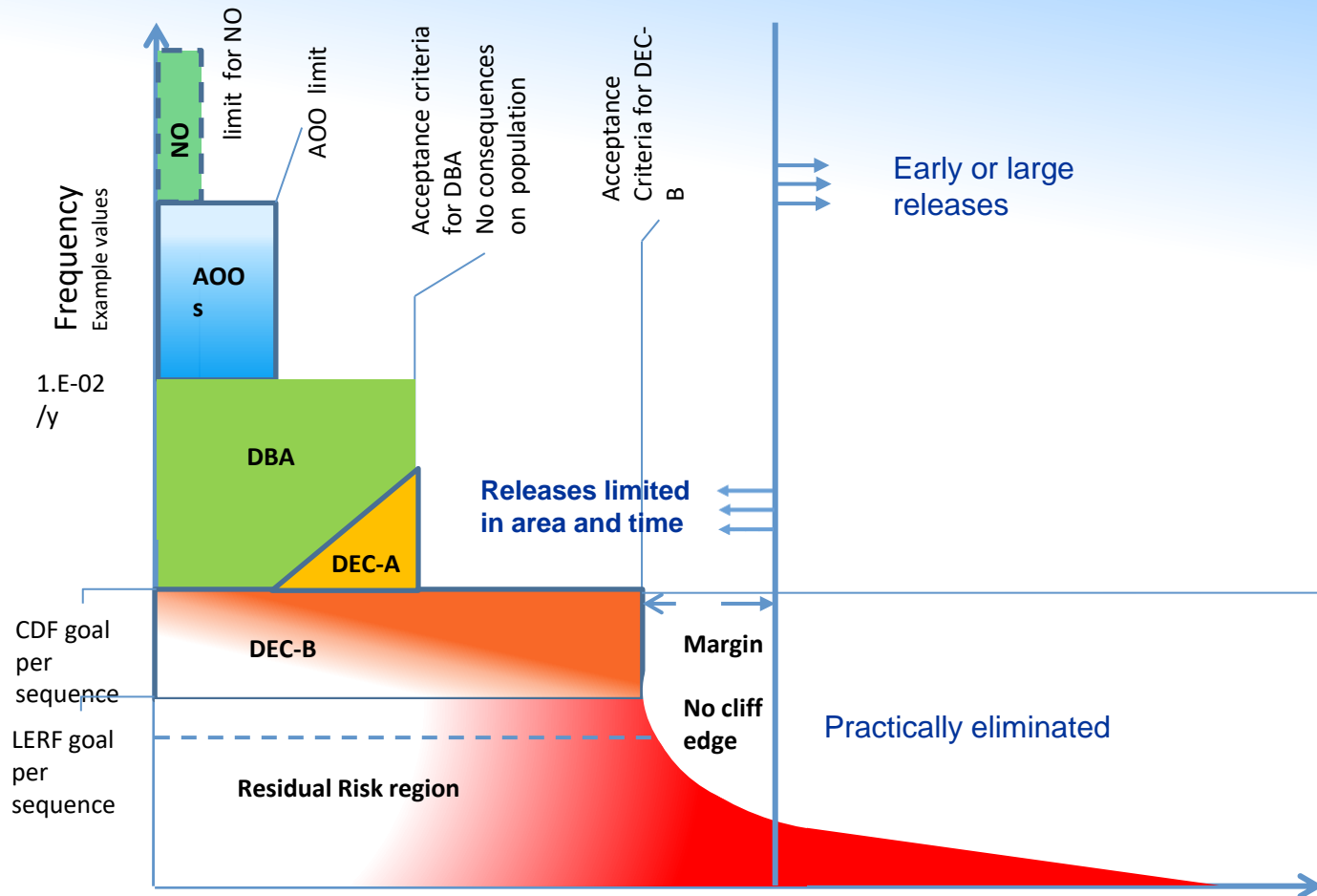
## Earlier Concept



## SSR-2/1, 2012







**Illustration of Plant State Frequencies vs. Consequences and Acceptance Criteria**



# Practical Elimination & Plant States

← Plant design envelope →

Operational states		Accident conditions	
NO	AOO	DBAs	Design Extension Conditions
			Without significant fuel degradation
			With core melting (severe accidents)
Loads and conditions generated by External & Internal Hazards (for each plant state)			
Criteria for functionality, capability, margins, layout and reliability (for each plant state)			
Design basis of equipment for Operational states	Design Basis of Safety Systems including SSCs necessary to control DBAs and some AOOs	Design Basis of safety features for <u>DECs</u> including SSCs necessary to control DECs	
		Features to prevent core melt	Features to mitigate core melt (Containment systems)

# Conclusion

## The IAEA Specific Safety Requirements – Safety of Nuclear Power Plants: Design SSR-2/1 (Rev. 1)

- **Reflects the international consensus on what constitutes a high level of safety that can reasonably be achieved in the design of nuclear power plants, to meet the fundamental safety objective and in compliance with the ten safety principles**
- **Defence in depth concept constitutes the primary means of preventing accidents in a nuclear power plant and mitigating the consequences of accidents if they do occur.**
- **The correct implementation of both the practical elimination concept and the defence in depth ensures the achievement of the fundamental safety objective.**
- **The justification of practical elimination of plant event sequences should rely on the demonstration of the physical impossibility or on the demonstration that it can be considered with a high degree of confidence to be extremely unlikely to arise.**



**IAEA**

International Atomic Energy Agency  
*Atoms for Peace and Development*



*Thank you for your attention!*  
*Questions?*

[J.Luis-Hernandez@iaea.org](mailto:J.Luis-Hernandez@iaea.org)