Training Course
on the IAEA Safety Standards Overview

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

Shahen POGHOSYAN

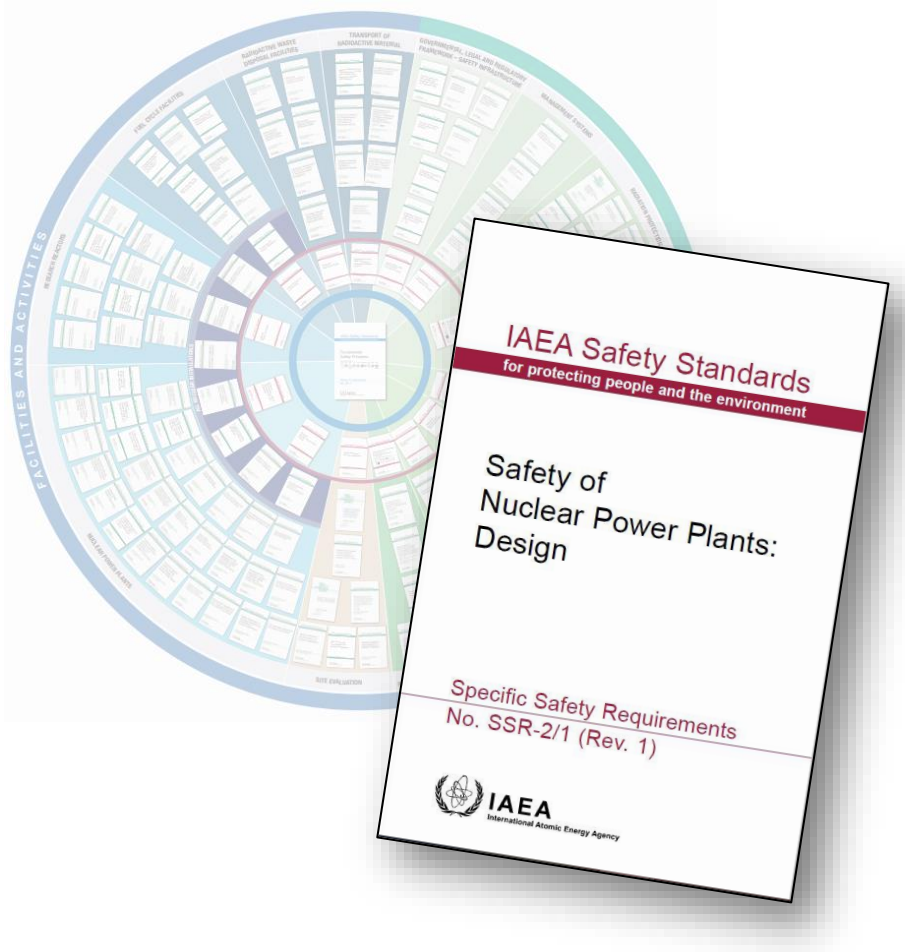
Safety Assessment Section (SAS)
Division of Nuclear Installation Safety (NSNI)
Department of Nuclear Safety and Security, IAEA

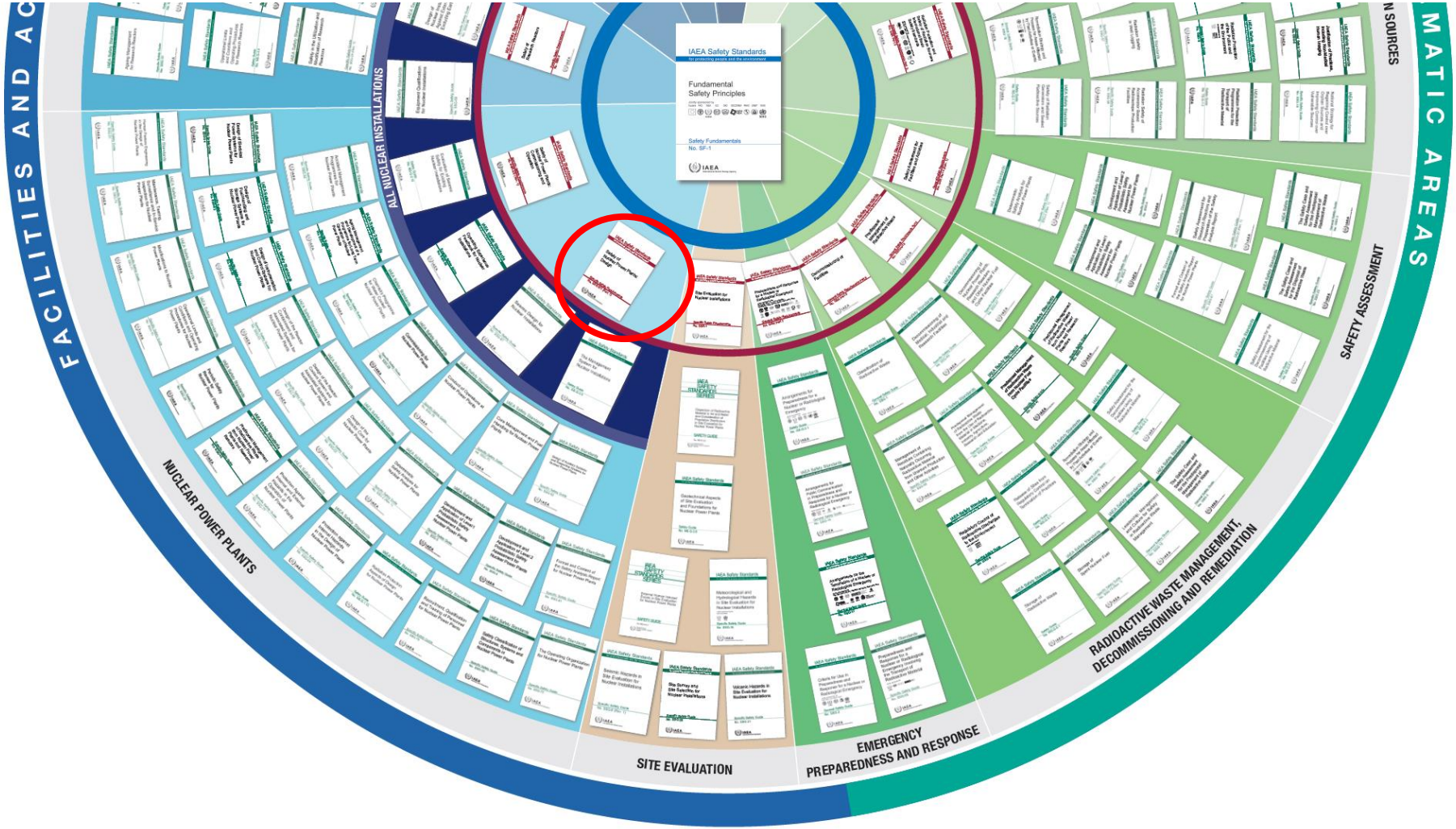
Shinagawa Campus, Tokai University, Tokyo, Japan

17-19, 21 March 2025

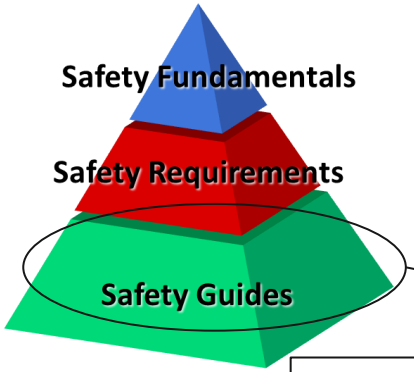
Outline

- INTRODUCTION
- REV.1 OF IAEA DESIGN SAFETY REQUIEMENTS
- OVERVIEW OF REQUIREMENTS
  - MANAGEMENT OF SAFETY IN DESIGN
  - PRINCIPAL TECHNICAL REQUIREMENTS
  - GENERAL PLANT DESIGN REQUIREMENTS
  - DESIGN OF SPECIFIC PLANT SYSTEMS
- CONCLUSIONS




IAEA Safety Standards
for protecting people and the environment
Fundamental Safety Principles
Safety Fundamentals
No. SF-1
IAEA
ALL NUCLEAR INSTALLATIONS
NUCLEAR POWER PLANTS
SITE EVALUATION
EMERGENCY PREPAREDNESS AND RESPONSE
RADIOACTIVE WASTE MANAGEMENT, DECOMMISSIONING AND REMEDIATION
SAFETY ASSESSMENT
N SOURCES
MATIC AREAS
FACILITIES AND AC

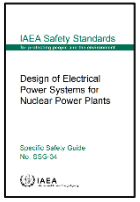
Design Safety

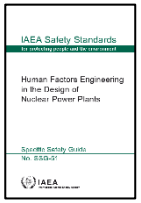


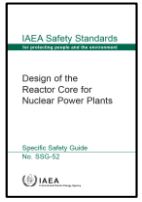
Safety objectives and safety principles

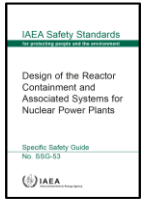
Functional conditions required for safety

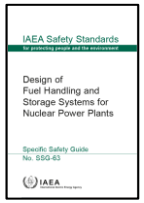
Guidance on how to fulfil the requirements

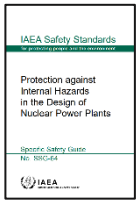


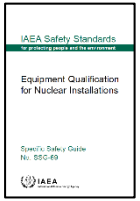


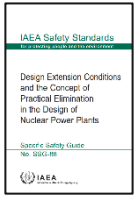


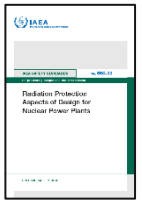












Safety approach for the design of NPPs

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**

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

- **Published in 2016**, revised **after 2012** 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 **wide range of stakeholders**: 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

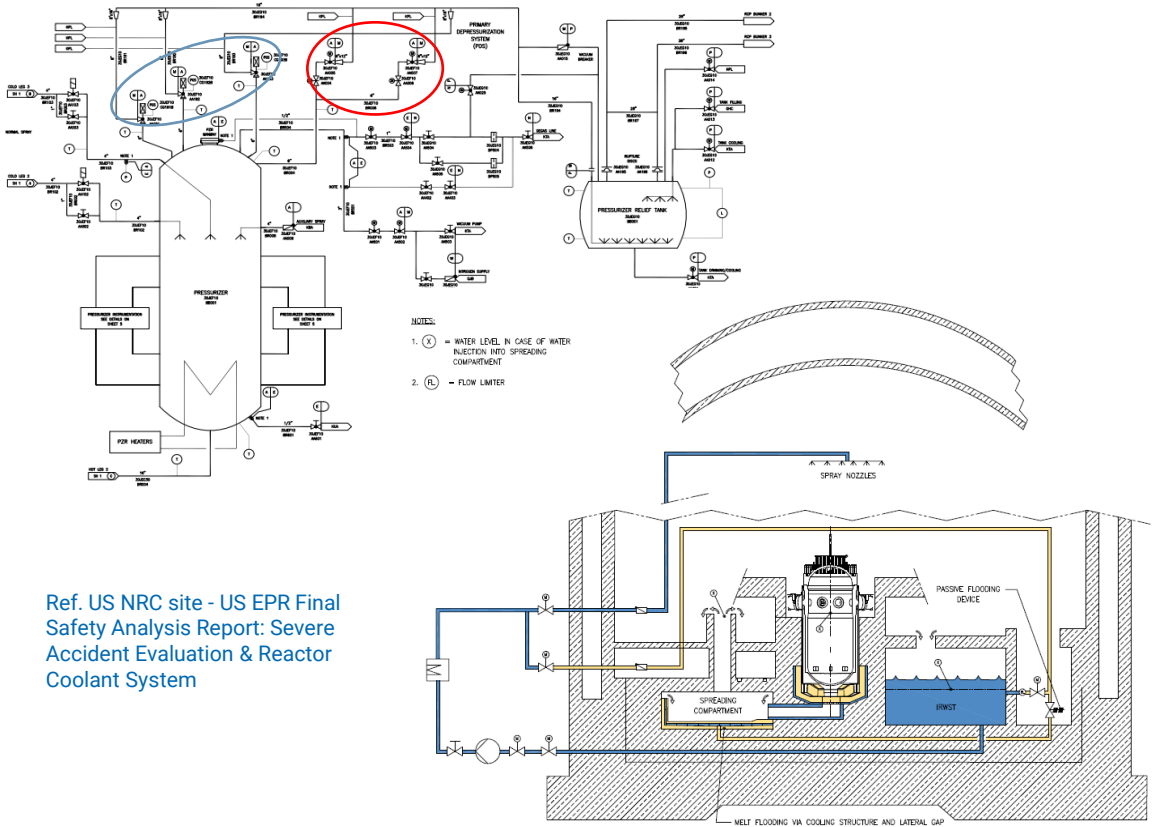
- taking into consideration impact of site on design
- ensuring safe operation and maintenance of plant

Importance of SSR for NPP Design (2/2)

Requirements collected in this safety standard

- are the main reference to perform IAEA 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)



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

Reinforce the **application of the Defence-in-Depth concept**, by implementing independent Defence-in-Depth provisions

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

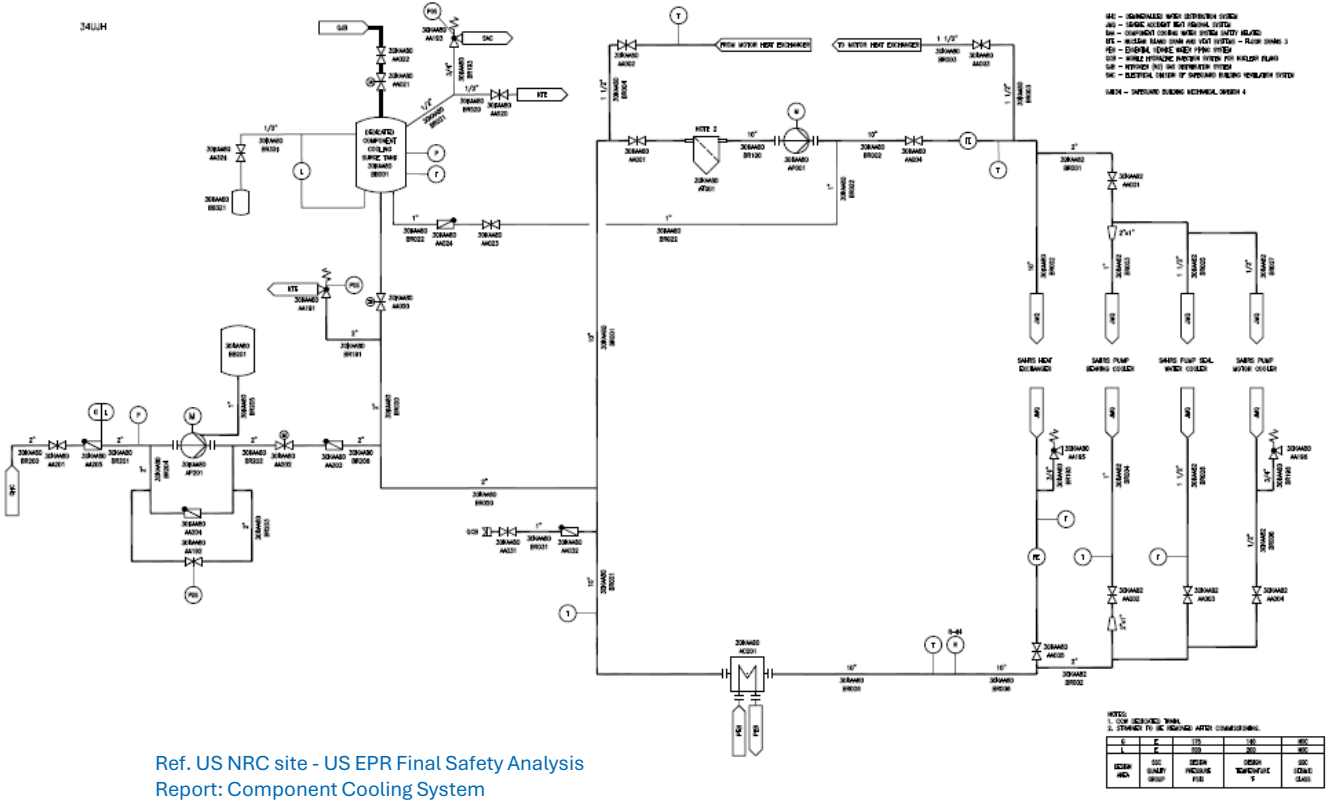
Multi-unit site considerations related to the independence of dedicated, to each unit, safety systems for DBA and additional safety features for DEC.

DBA=Design Basis Accidents

DEC=Design Extension Conditions

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

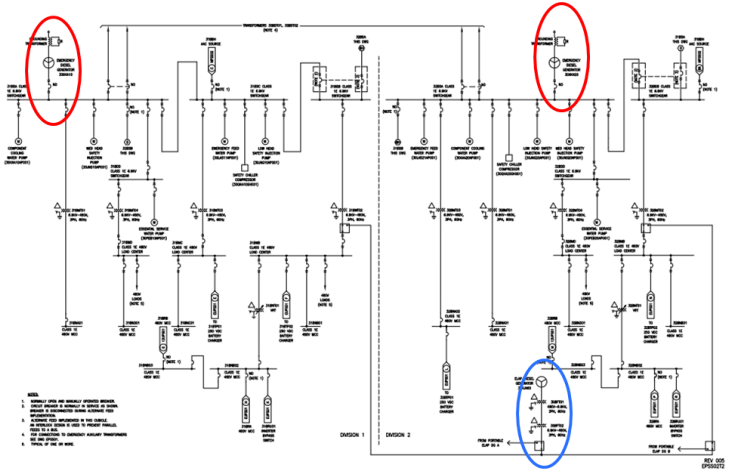
Reinforced capabilities for heat transfer to the UHS. Alternative heat sink or different access is required if heat transfer cannot be ensured in conditions generated by hazards more severe than those selected for the design basis



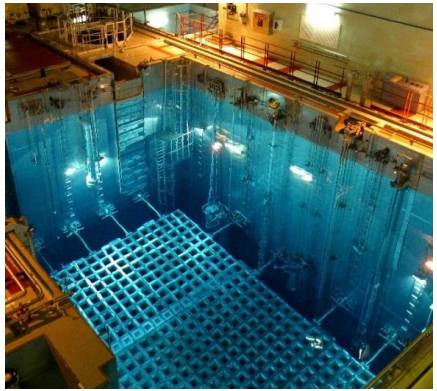
UHS=Ultimate Heat Sink

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)



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



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

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

CONTENTS

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

Design safety

Management of Safety in Design Requirements

Management of Safety in Design

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

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

Requirement 2: Management system for plant design

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

Management of Safety in Design

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

- The **operating organization** shall establish a formal system for ensuring the continuing safety of the plant design throughout the lifetime of the nuclear power plant.
- It shall be ensured that
  - the plant design meets the acceptance criteria for safety, reliability and quality as defined in plant design, and verified during the periodic safety reviews
  - formal system is established for
    - design verification,
    - definition of engineering codes and standards and requirements,
    - use of proven engineering practices,
    - provision for feedback of information on construction and experience,
    - approval of key engineering documents,
    - conduct of safety assessments and maintaining a safety culture

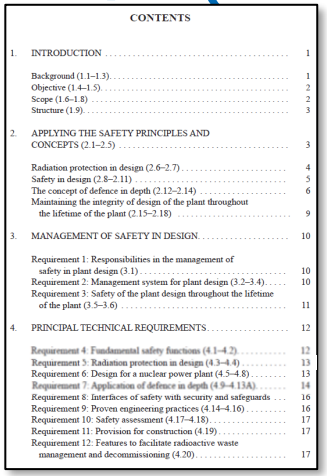
Management of Safety in Design

Requirement 3:

- the knowledge of the design is available and maintained up to date
- management of design requirements and configuration control are maintained
- necessary interfaces with responsible designers and suppliers engaged in design work are established and controlled
- engineering expertise and scientific and technical knowledge are maintained within the operating organization
- design changes to the plant are reviewed, verified, documented and approved
- adequate documentation is maintained to facilitate future decommissioning of the plant

Design safety
Principal Technical Requirements
& General plant design

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



CONTENTS

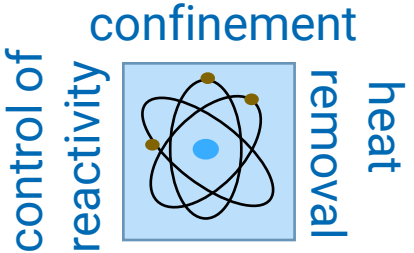
Requirement 5: Radiation Protection in Design

Requirement 4: Fundamental Safety Functions

Requirement 13: Categories of Plant States

Requirement 14: DB for items important to Safety

Requirement 7: Application of Defence in Depth



Design safety
Principal Technical Requirements
& General plant design

5 ‘key’ requirements 🖐

Requirement 5: Radiation protection

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

- do not exceed authorized limits and are kept as low as reasonably achievable in **normal operation and anticipated operational occurrences and during decommissioning**, and
- remain below acceptable limits **during and following accident conditions**.
- The design shall be such as to ensure that plant states that could lead to **high radiation doses or large radioactive releases are practically eliminated** and that there are no, or only minor, potential radiological consequences for plant states with a significant likelihood of occurrence.
- Acceptable limits for radiation protection associated with the relevant categories of plant states shall be established, consistent with the regulatory requirements.

Requirement 4: Fundamental safety functions (FSF)

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

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

A systematic approach shall be taken to identifying those **items important to safety** that are necessary to fulfil the FSFs functions and to identifying the inherent features that are contributing to fulfilling, or that are affecting the FSFs

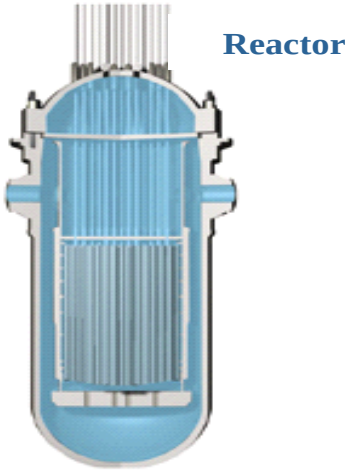
Means of **monitoring the status of the plant** shall be provided for ensuring that the required safety functions are fulfilled.

An item that is part of a safety group and/or whose malfunction or failure could lead to radiation exposure of the site personnel or members of the public

Requirement 4: Fundamental safety functions (examples)

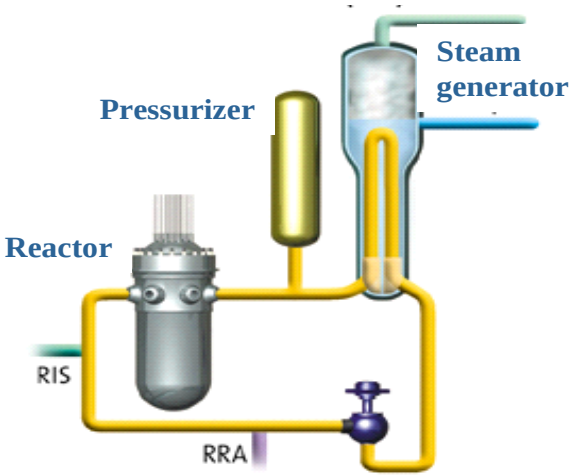
Control of reactivity

- Control rods
- Boron injection



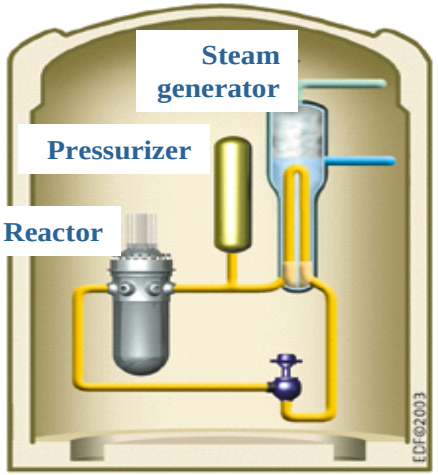
Cooling of the core

- Steam generators
- Residual hear removal
- Safety injection



Confinement of radioactive materials

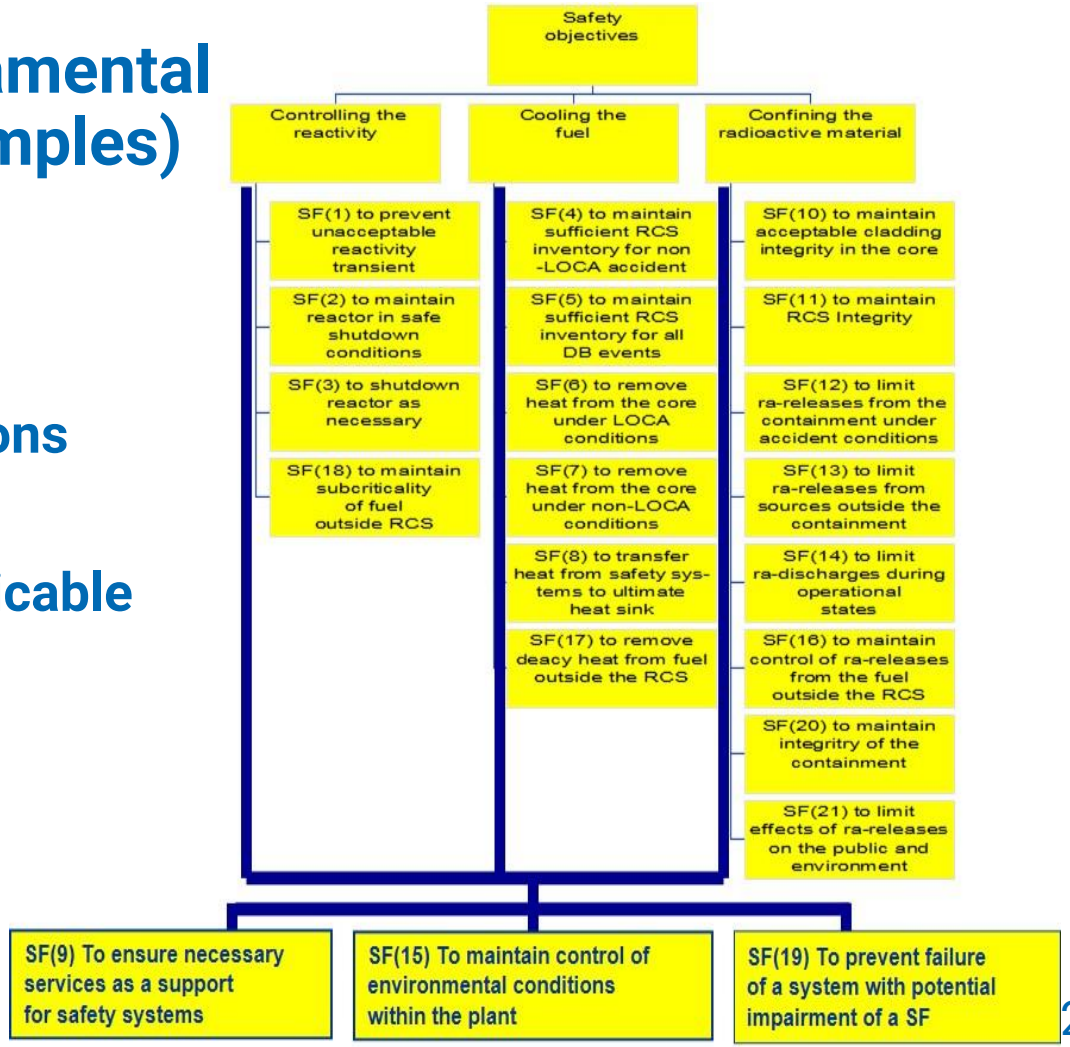
- Fuel cladding
- Primary cooling system
- Containment



Requirement 4: Fundamental safety functions (examples)

Fundamental safety functions

Derived safety functions applicable for LWRs



Requirement 7: Application of defence in depth

From SF-1, principle 8

The primary means of preventing and mitigating the consequences of accidents is '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.

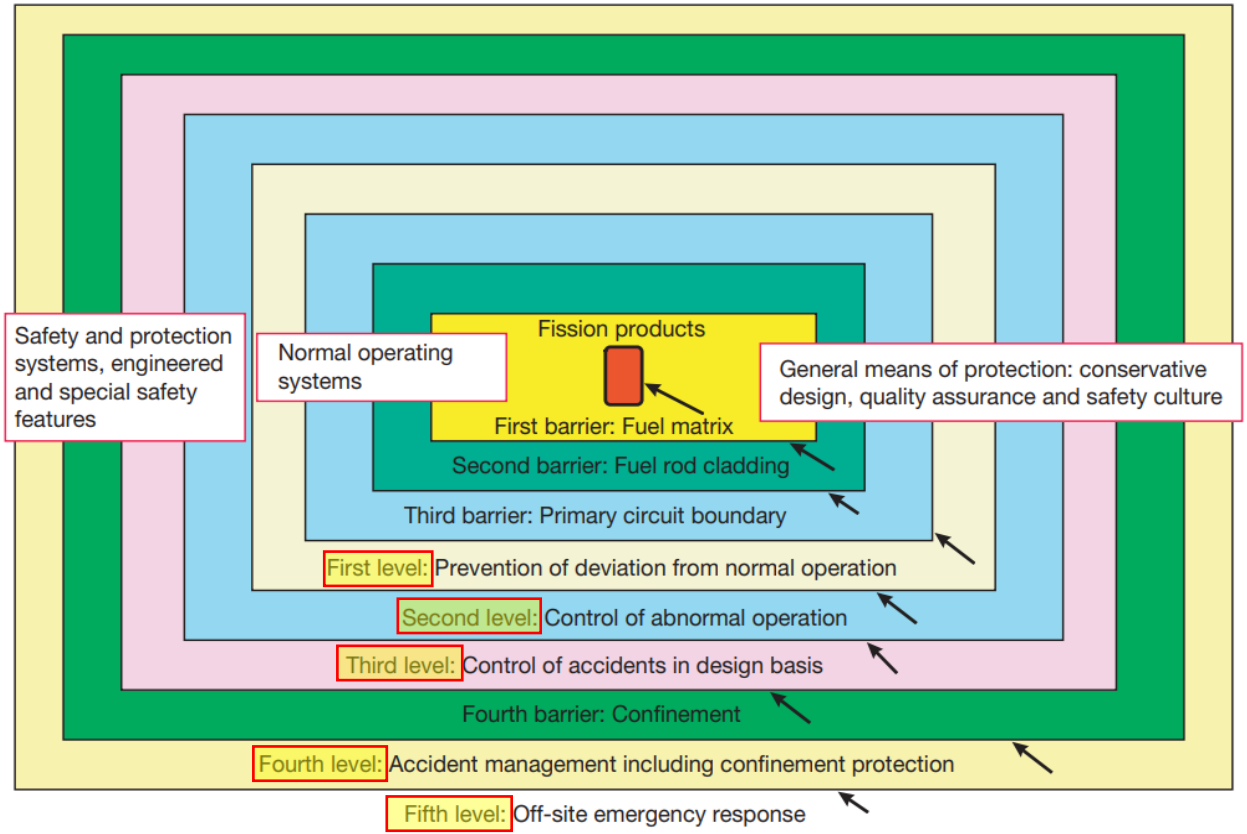
- The existence of multiple levels of defence is not a basis for continued operation in the absence of one level of defence. All levels of defence in depth shall be kept available at all times.
- Relaxations shall be justified for specific modes of operation

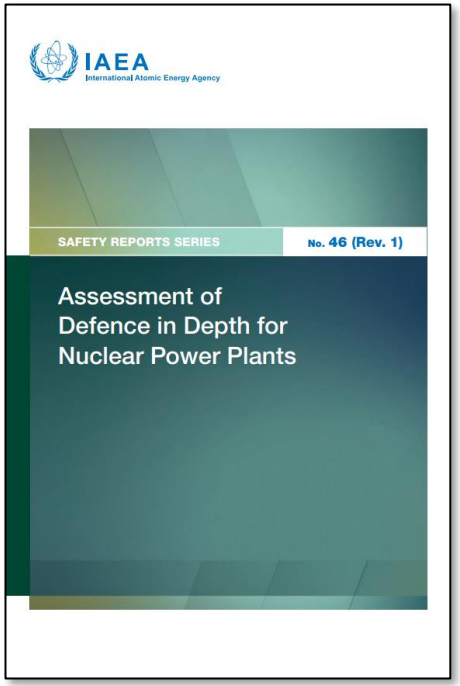
Requirement 7: Application of defence in depth

The design shall

- provide for **multiple physical barriers** to the release of radioactive material;
- **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;
- 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;
- 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**;
- 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;**
- provide **multiple means for ensuring** that each of the **fundamental safety functions** is performed, thereby ensuring the effectiveness of the barriers

Requirement 7: Application of defence in depth





Requirement 7: Application of defence in depth

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

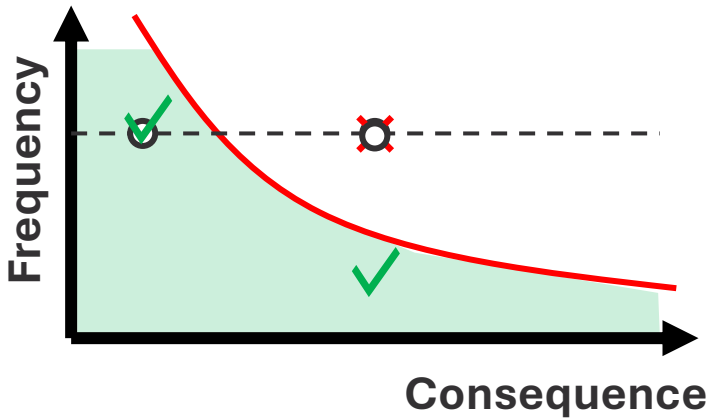
- The levels of defence in depth **shall be independent as far as practicable** to avoid a failure of one level reducing the effectiveness of other levels. In particular, safety features for design extension conditions (especially features for mitigating the consequences of accidents involving the melting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

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;
- Design basis accidents;
- Design extension conditions, including accidents with core melting.

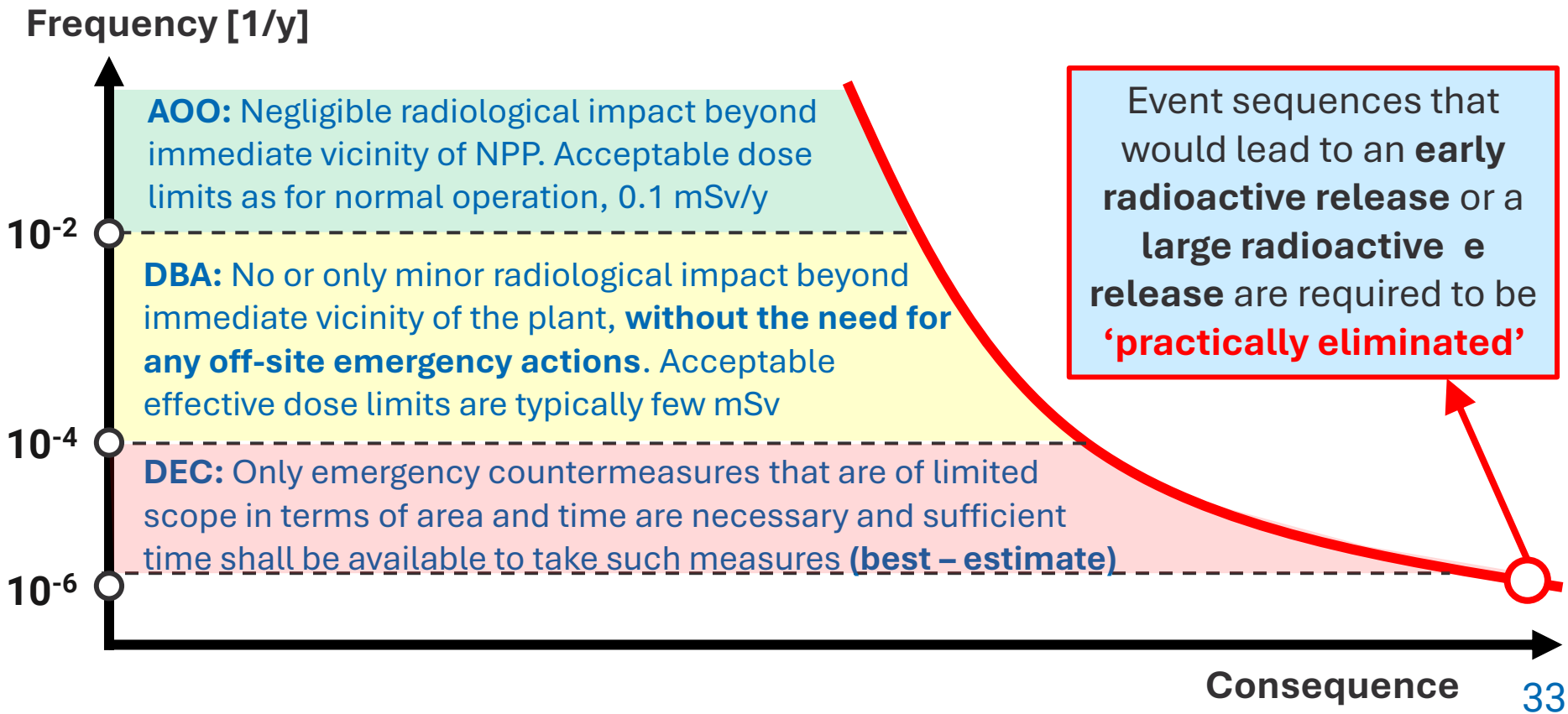
Criteria shall be assigned to each plant state, such that **frequently occurring plant states shall have no, or only minor, radiological consequences** and plant states that could give rise to serious consequences shall have a very low frequency of occurrence.



Requirement 13: Categories of plant states

	Frequency (f) range Examples [per year]
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.**	**> 10^{-2}**
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.**	**10^{-2}-10^{-4}**
Design Extension Conditions (DECs) Postulated accident conditions **that are not considered for design basis accidents**, but that are considered in the design process of the facility in accordance **with best estimate methodology, and for which releases of radioactive material are kept within acceptable limits.** DEC could include conditions without significant fuel degradation and conditions with core melting.	**10^{-4}-10^{-6}** *(no core melt)* **10^{-6} >** *(with core melt)*

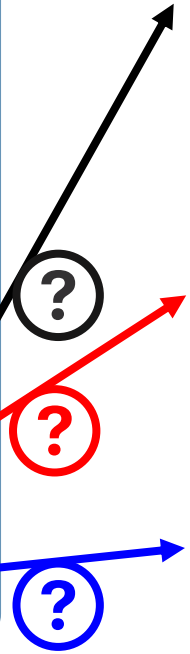
Requirement 13: Categories of plant states



Practical elimination

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**

Requirement 14: Design basis for items important to safety

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

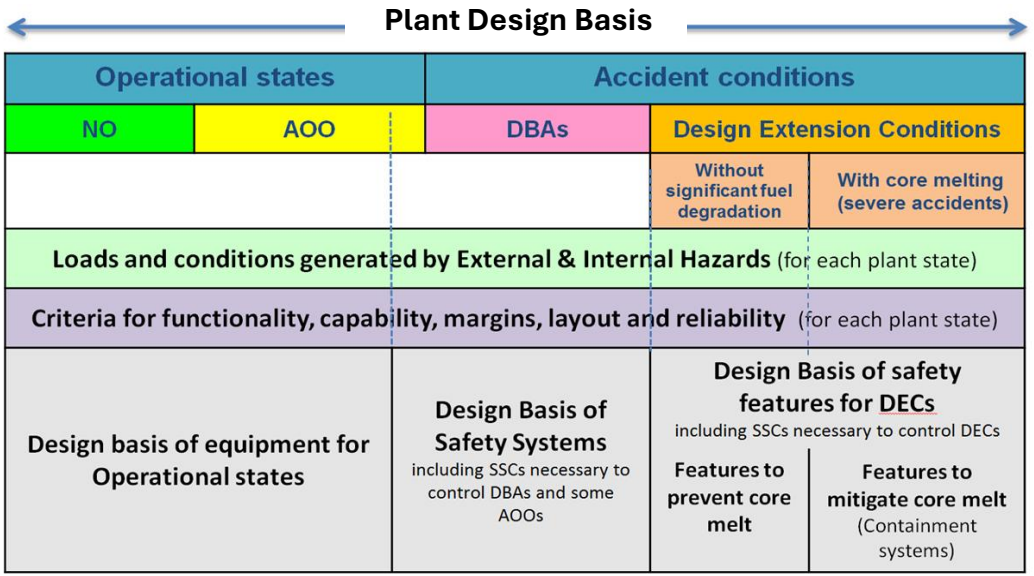
The design basis for each item important to safety **shall be systematically justified and documented.**

Design basis of the plant (e.g. it is a design basis accident) means in reality that the conditions generated due to a given accident are included in the design basis of a set of structures, systems and components (SSCs) that have the function to deal with and control that accident.

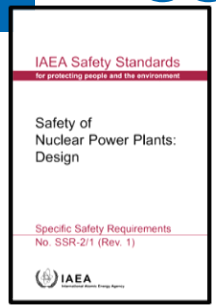
Requirement 14: Design basis for items important to safety

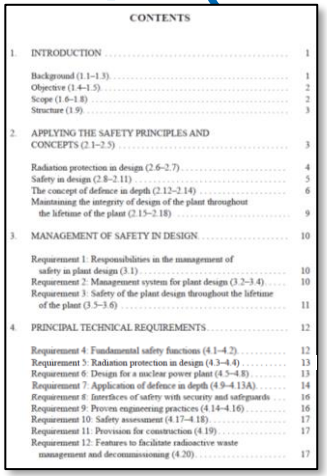
The design basis specifies for each structure, system and component (SSC) of the NPP:

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



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





CONTENTS

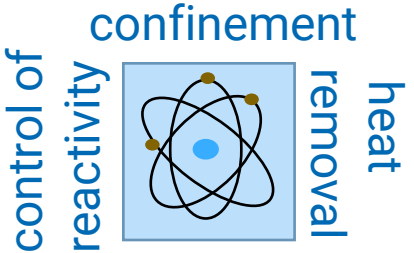
Requirement 5: Radiation Protection in Design

Requirement 4: Fundamental Safety Functions

Requirement 13: Categories of Plant States

Requirement 14: DB for items important to Safety

Requirement 7: Application of Defence in Depth



Design safety
Principal Technical Requirements
& General plant design

Other important requirements 😎

Requirement 9: Proven engineering practices

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

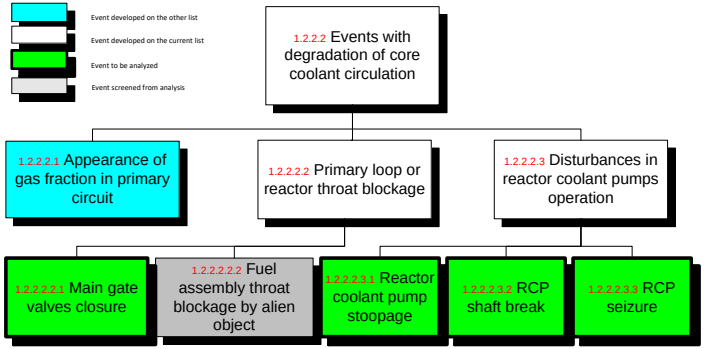
- Items important to safety shall preferably be of a design that has **previously been proven**
- If not, shall be items of **high quality and of a technology** (qualified and tested)
- **If unproven design or feature is introduced** or if there is a departure from an established engineering practice, safety shall be demonstrated by means of
  - appropriate supporting research programmes,
  - performance tests with specific acceptance criteria
  - examination of operating experience from other relevant applications
  - monitor in service to verify the behaviour is as expected

Requirement 16: Postulated initiating events

Design shall apply a systematic approach to identifying a comprehensive set of postulated initiating events such that all foreseeable events with the potential for serious consequences and with a significant frequency of occurrence are anticipated and are considered in the design. PIEs shall:

- be identified using **engineering judgement** and a combination of **deterministic** and **probabilistic** considerations.
- include **all foreseeable failures of SSCs**, operating errors and failures arising from hazards
- cover **all operating states** (e.g. LPSD)
- be analysed to **establish the preventive measures and protective measures** that are necessary to ensure performance of the safety functions

Component, train, system	Failure mode	Effect
Fan 1V-36	Failure to operate	Decrease of V-36 vent system reliability
Fan 1V-36	Failure on demand	Decrease of V-36 vent system reliability
Fan 1V-36	Unavailability due to repair	Decrease of V-36 vent system reliability
...	...	...



Requirement 17: Internal and external hazards

- All foreseeable **internal hazards and external hazards**, including the potential for human induced events to affect the safety of NPP, shall be identified and their effects shall be evaluated.
- Hazards shall be considered in designing the layout of the plant and in **determining the PIEs and generated loadings** for use in the design of relevant items important to safety for the plant.
- Items important to safety shall be designed and located **to withstand the effects of hazards or to be protected, in accordance with their importance to safety,** against hazards and against common cause failure mechanisms generated by hazards.
- For **multiple unit plant sites**, the design shall take due account of the potential for specific hazards to give rise to impacts on several or even all units on the site simultaneously.

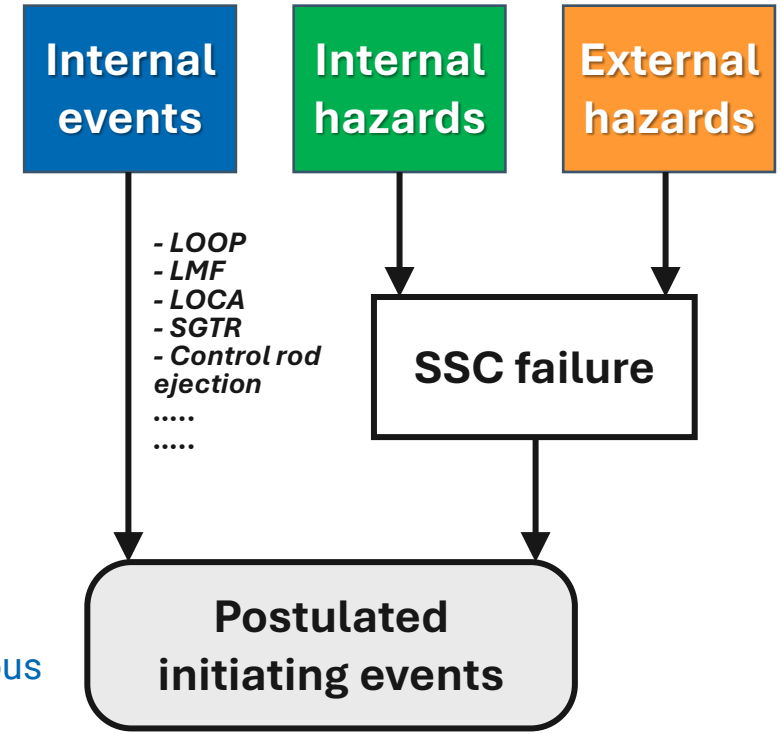
Requirement 17: Internal and external hazards

Internal hazards

- Fire
- Explosion
- Flooding
- Missile generation
- Collapse of structures and falling objects
- Pipe whip
- Jet impact
- Release of fluid from failed systems or from other installations on the site

External hazards

- Natural
  - Earthquake
  - Tsunami
  - Volcano eruption
  - Flooding
  - Extreme weather conditions
  - …
- Human induced
  - Aircraft impact
  - Explosions
  - Fire
  - Release of Hazardous Substances
  - …

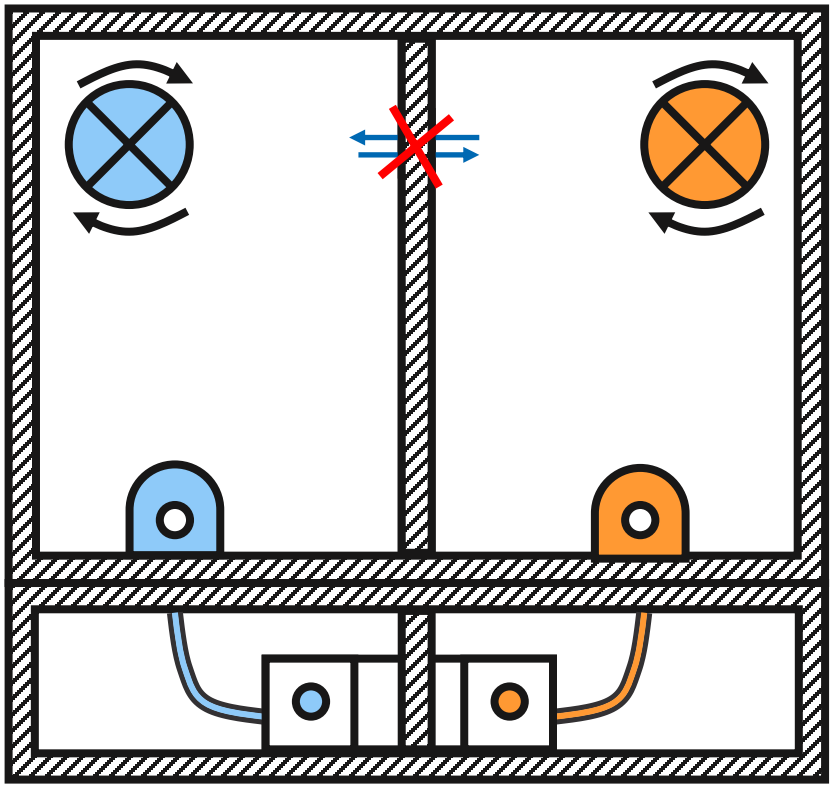


Requirements 21: Physical separation and independence of safety systems

Interference between safety systems or between redundant elements of a system shall be prevented by means such as

- physical separation,
- electrical isolation,
- functional independence
- independence of communication (data transfer)

as appropriate.



Requirements 22: Safety classification

All items important to safety shall be identified and shall be classified on the basis of their function and their safety significance.

The method for classification shall be based primarily on deterministic methods complemented, where appropriate, by probabilistic methods, taking into account factors e.g.:

- **Safety function** (SF) to be performed by the item
- **Consequences** of failure to perform a SF;
- **Frequency** with which the item will be called upon to perform a safety function;
- **Time** following a postulated initiating event at which, or the period for which, the item will be called upon to perform a safety function.

TABLE 1. RELATIONSHIP BETWEEN FUNCTIONS CREDITED IN THE ANALYSIS OF POSTULATED INITIATING EVENTS AND SAFETY CATEGORIES

Functions credited in the safety assessment	Severity of the consequences if the function is not performed		
	High	Medium	Low
Functions to reach a controlled state after anticipated operational occurrences **AOO**	Safety category 1	Safety category 2	Safety category 3
Functions to reach a controlled state after design basis accidents **DBA**	Safety category 1	Safety category 2	Safety category 3
Functions to reach and maintain a safe state	Safety category 2	Safety category 3	Safety category 3
Functions for the mitigation of consequences of design extension conditions **DEC**	Safety category 2 or 3 (see para. 3.15)	Not categorized [a]	Not categorized [a]

[a] Medium or low severity consequences are not expected to occur in the event of non-response of a dedicated function for the mitigation of design extension conditions.

IAEA SSG-30

Requirement 10: Safety Assessment

- **Comprehensive deterministic safety assessments and probabilistic safety assessments shall be carried out throughout the design process** for a nuclear power plant to ensure that all safety requirements on the design of the plant are met throughout all stages of the lifetime of the plant, and to confirm that the design, as delivered, meets requirements for manufacture and for construction, and as built, as operated and as modified.
- **The safety assessments shall be commenced at an early point in the design process**, with iterations between design activities and confirmatory analytical activities, and shall increase in scope and level of detail as the design programme progresses.
- The safety assessments shall be documented in a form that facilitates **independent evaluation.**

Requirement 42: Safety analysis of the plant design

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

The safety analysis shall provide assurance that:

- **design basis are confirmed** for items important to safety and their links to initiating events and event sequences
- NPP is capable of complying with **authorized limits on discharges with regard to radioactive releases and with the dose limits in all operational states**
- NPP is capable of meeting **acceptable limits for accident conditions**.
- DiD has been implemented
- uncertainties adequately considered and adequate margins are available to **avoid cliff edge effects** and **early radioactive releases or large radioactive releases**.
- analytical assumptions, methods and degree of conservatism used in the design of the plant shall be updated and verified for the current or as built design.

Requirement 8: 3S interfaces

Requirement 8: Interfaces of safety with security and safeguards

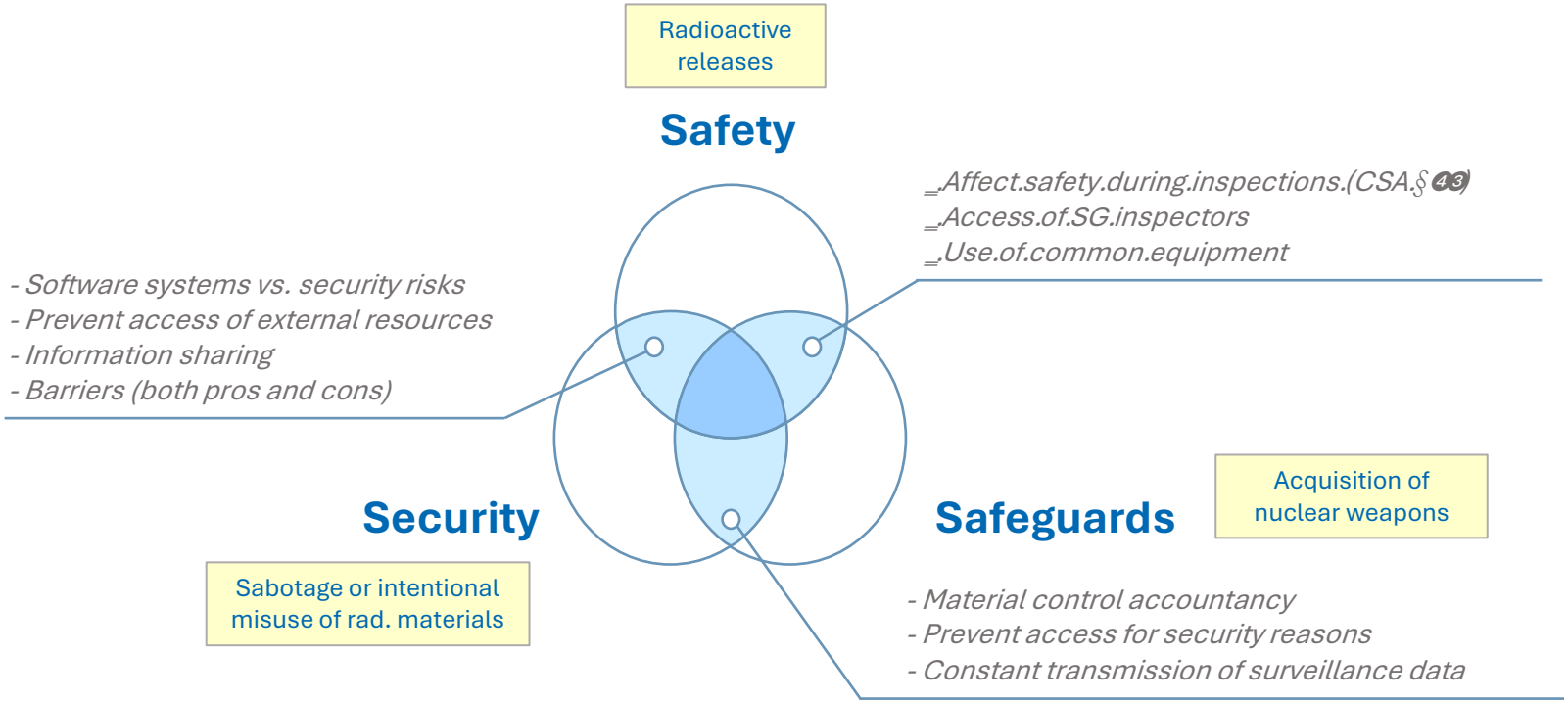
Safety measures, nuclear security measures and arrangements for the State system of accounting for, and control of, nuclear material for a nuclear power plant shall be designed and implemented in an integrated manner so that they do not compromise one another.

- **There are interfaces** between 3S (conflicts, potential synergies)
- Interfaces are currently **not considered systematically**
- **Hard to address** (or impossible) when design is finalized
- **Unique time window** while the reactors are in design stage
- **Getting more complex** in light of the innovative reactors, e.g. SMRs (novelties lead to several challenges for all 3S)

How the design process goes in reality

☺ Joking!

Requirement 8: 3S interfaces



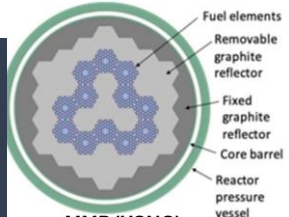
SMR Novelties vs challenges for 3S

- Transportability
- Locations (remote, urban)
- New fuel concepts
- Long refueling periods
- Higher enrichment
- Factory sealed cores
- Highly integrated software-based systems

2-3.5MW eVinci (WEC)

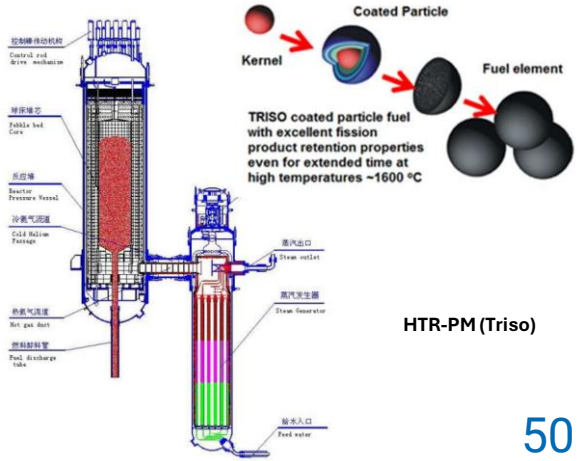
1.5-MW Aurora

RITM-200M
(up to 120months)



MMR (USNC)

35MW KLT-40S



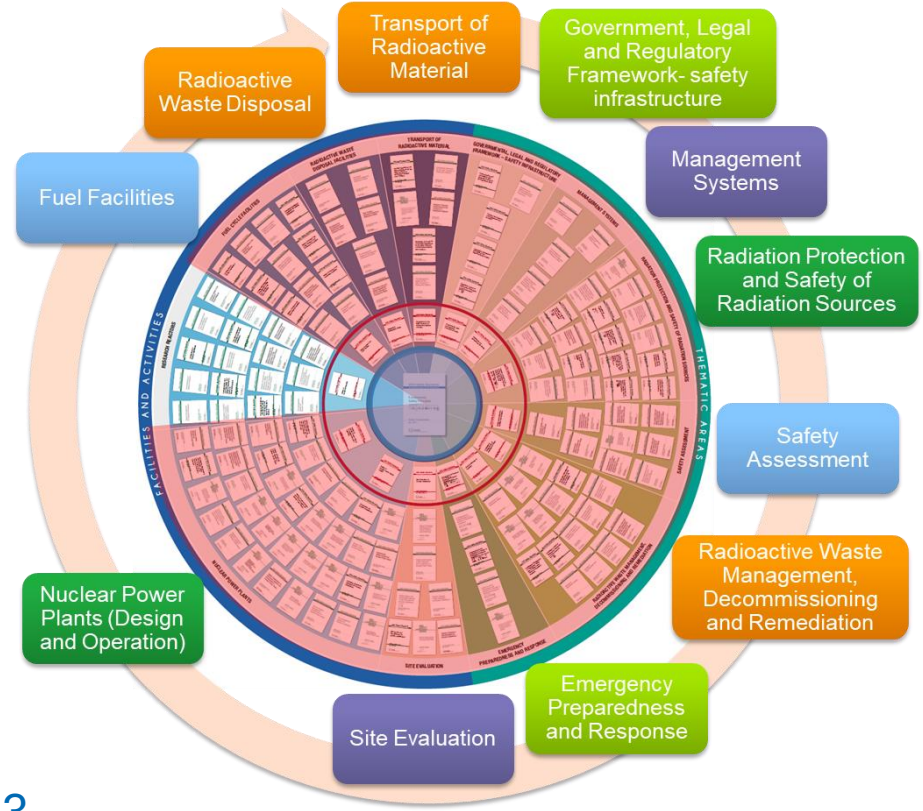
HTR-PM (Triso)

Applicability to non-water cooled reactors and SMRs

IAEA SSR-2/1(Rev.1): Applicability

- **Example from SSR-2/1(Rev.1) Scope**
  - 1.6. It is expected that this publication will be used primarily for land based stationary nuclear power plants with water cooled reactors designed for electricity generation or for other heat production applications (such as district heating or desalination). This publication may also be applied, with judgement, to other reactor types, to determine the requirements that have to be considered in developing the design.

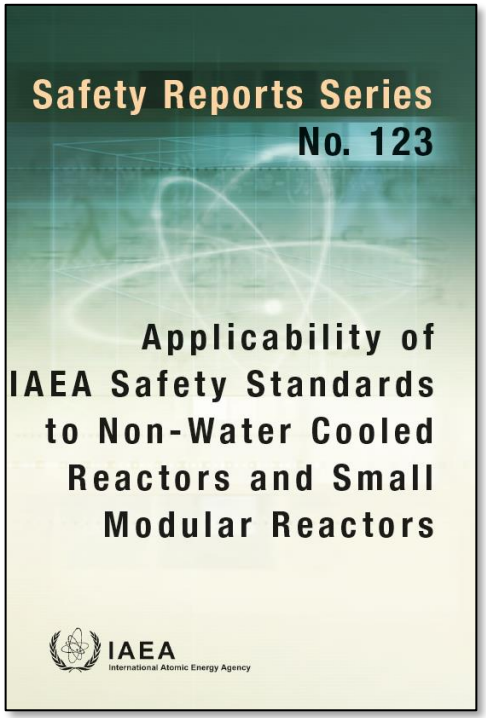
Review of applicability of Safety Standards to non-water cooled reactors and SMRs



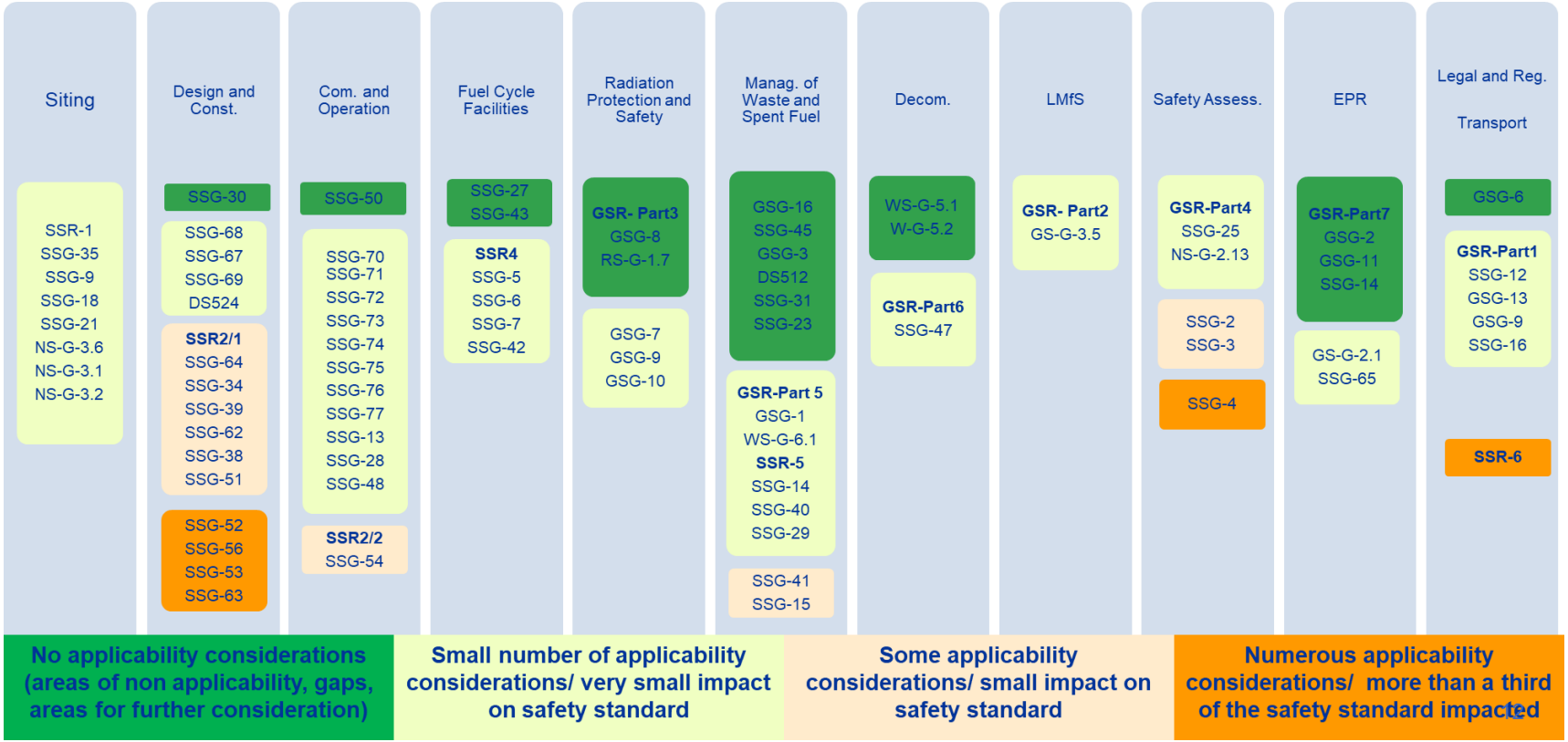
Are Safety Standards sufficient and relevant to ensure the safety of SMRs and Non Water Cooled Reactors?

Review of applicability of Safety Standards to non-water cooled reactors and SMRs

- **Various technologies were covered**
  - including small modular reactors (SMRs), high temperature gas cooled reactors (HTGRs), sodium fast reactors (SFRs), lead fast reactors (LFRs), molten salt reactors (MSRs), marine-based SMRs and micro-sized reactors
- **>150** international experts, from **30** Member States and **40** organisations
- Regulatory bodies, designers, technical support organisations, R&D



Applicability review summary outcomes



Concluding remarks

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
- **Contains 82 requirements:** Management of safety in design, Principal technical requirements, General plant design requirements, Design of specific plant systems
- **Key set of requirements** to for the design of the NPP
- **Supported by numerous Safety Guides:** e.g. system specific (reactor core, I&C)
- **Next revision of SSR-2/1(Rev.1)** has been just initiated in March 2025

Thank you!

Safety-Standards.Contact-Point@iaea.org