IAEA
International Atomic Energy Agency
Atoms for Peace and Development

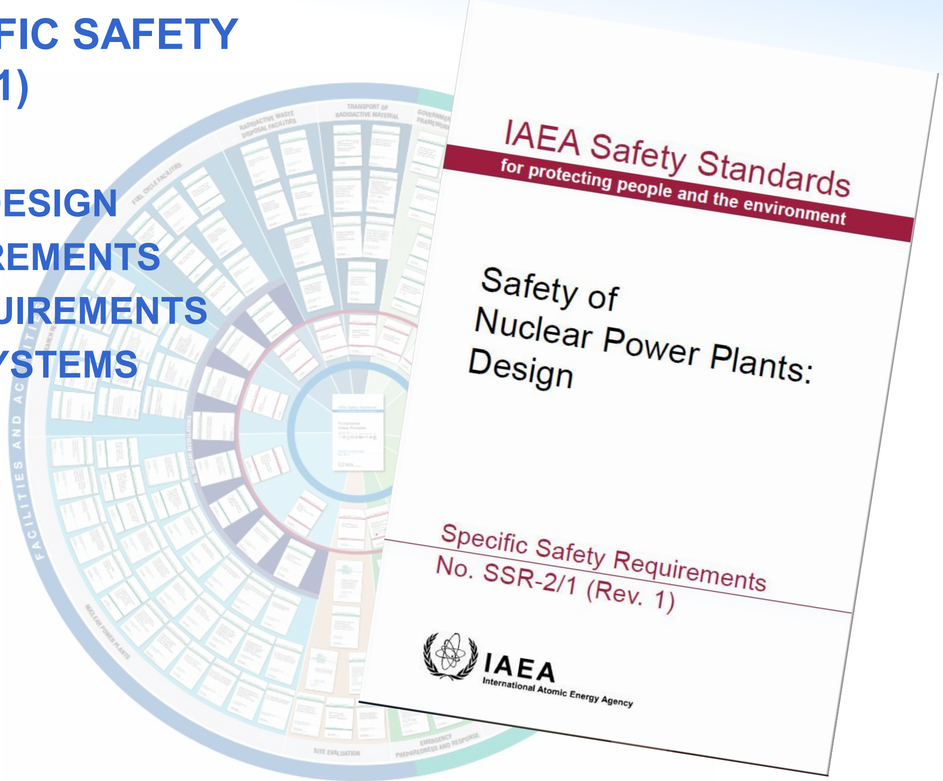
International Training Course on the IAEA Safety Standards at Tokai University, 11-14 March 2024

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

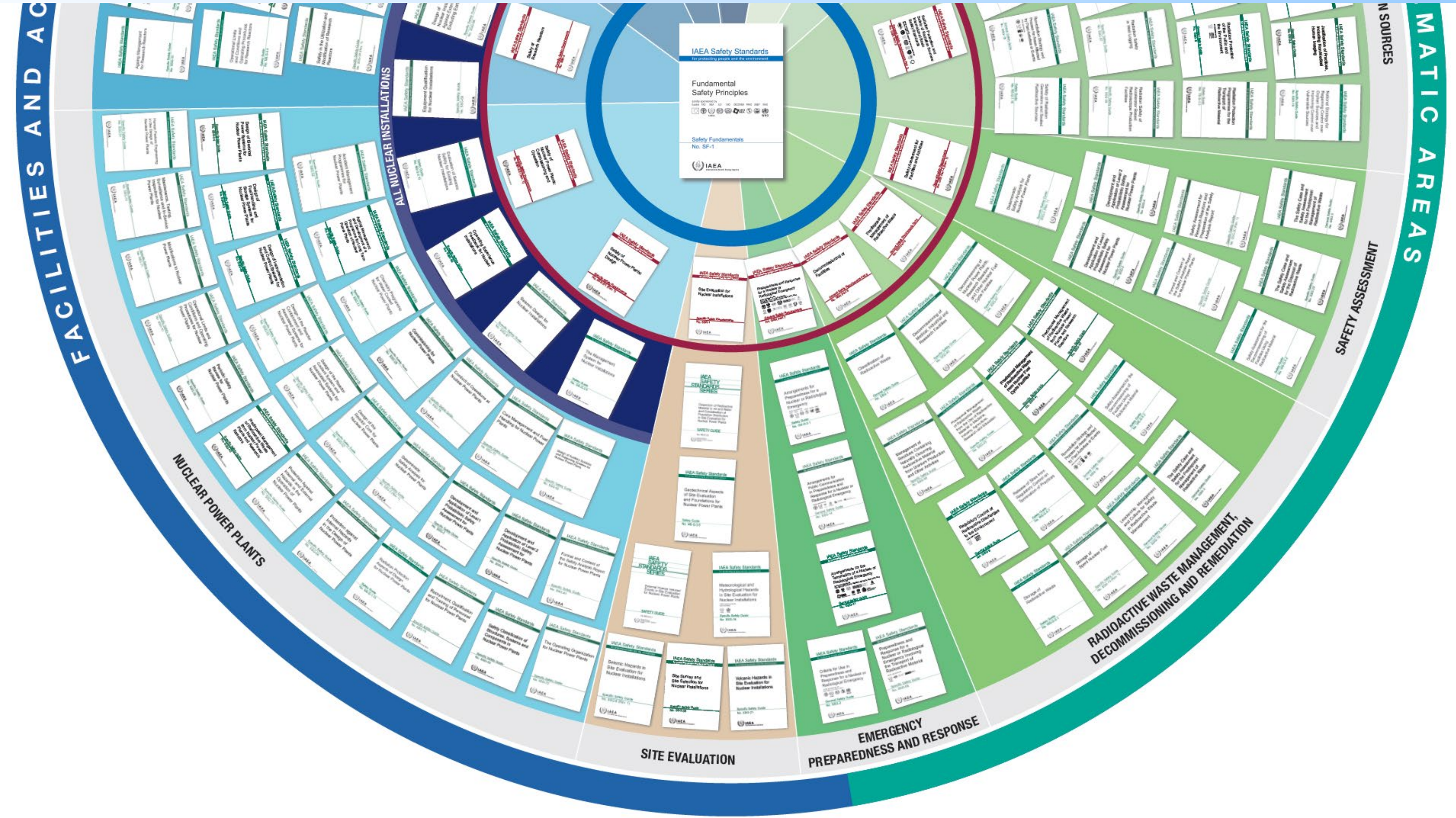
Jorge LUIS HERNANDEZ
Senior Nuclear Safety Officer (NPP Design Safety)
Safety Assessment Section (SAS), Division of Nuclear Installation Safety (NSNI)
Department of Nuclear Safety and Security
IAEA

Outline

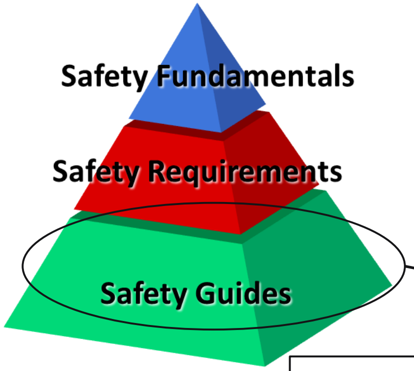
- DESIGN SAFETY
  - INTRODUCTION TO IAEA SPECIFIC SAFETY REQUIREMENTS SSR-2/1 (REV. 1)
  - OVERVIEW OF REQUIREMENTS
    - MANAGEMENT OF SAFETY IN DESIGN
    - PRINCIPAL TECHNICAL REQUIREMENTS
    - GENERAL PLANT DESIGN REQUIREMENTS
    - DESIGN OF SPECIFIC PLANT SYSTEMS
- CONCLUSIONS



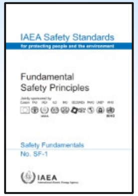
Design safety
Introduction to IAEA Specific Safety Requirements SSR-2/1 (Rev. 1)


IAEA Safety Standards
Fundamental Safety Principles
Safety Fundamentals No. SF-1
FACILITIES AND
ALL NUCLEAR INSTALLATIONS
NUCLEAR POWER PLANTS
SITE EVALUATION
EMERGENCY PREPAREDNESS AND RESPONSE
RADIOACTIVE WASTE MANAGEMENT, DECOMMISSIONING AND REMEDIATION
SAFETY ASSESSMENT
AREAS

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


IAEA Safety Standards
for protecting people and the environment

Safety of
Nuclear Power Plants:
Design

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

IAEA
International Atomic Energy Agency

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

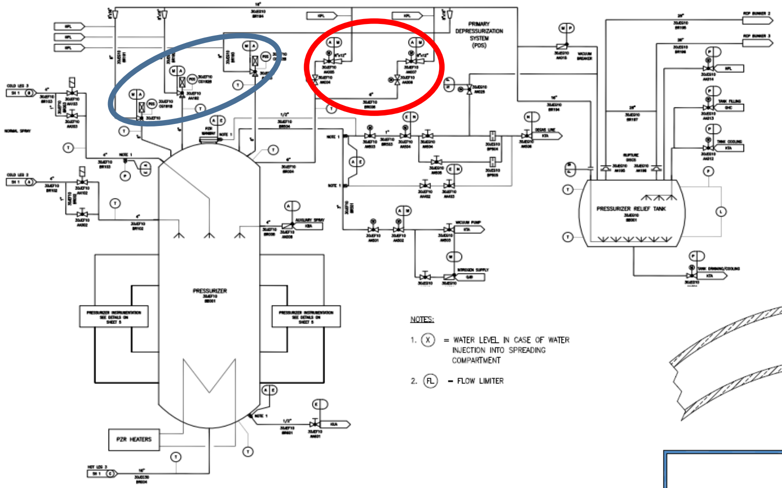
- taking into consideration impact of site on design
- ensuring safe operation and maintenance of plant

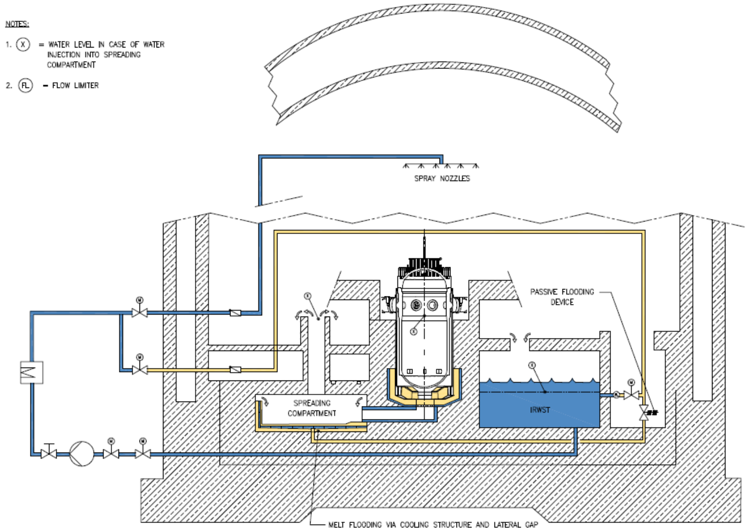
Importance of SSR for NPP Design (2/2)

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)





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, mainly between provisions required for levels 3 and 4

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

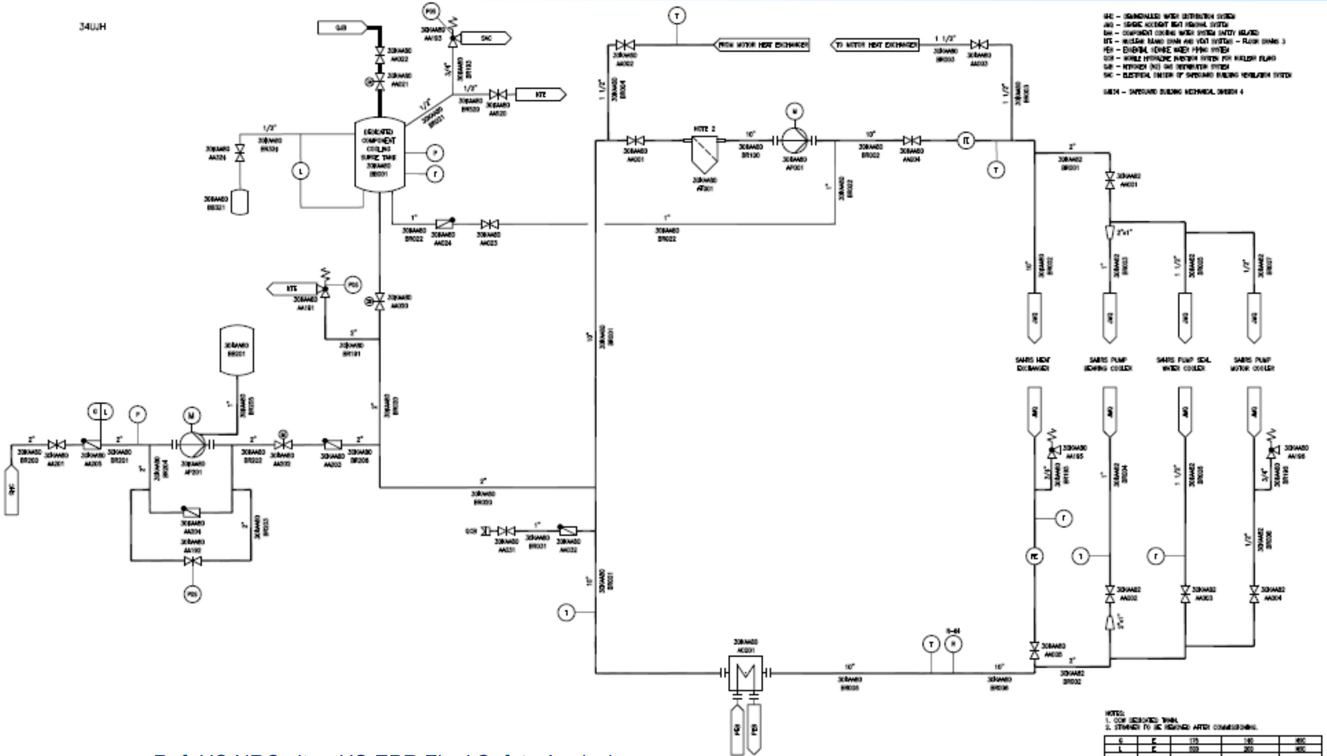
Multi-unit site considerations related to the independence of dedicated, to each unit, safety systems for DBA and additional safety features for DEC.

DBA=Design Basis Accidents

DEC=Design Extension Conditions

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

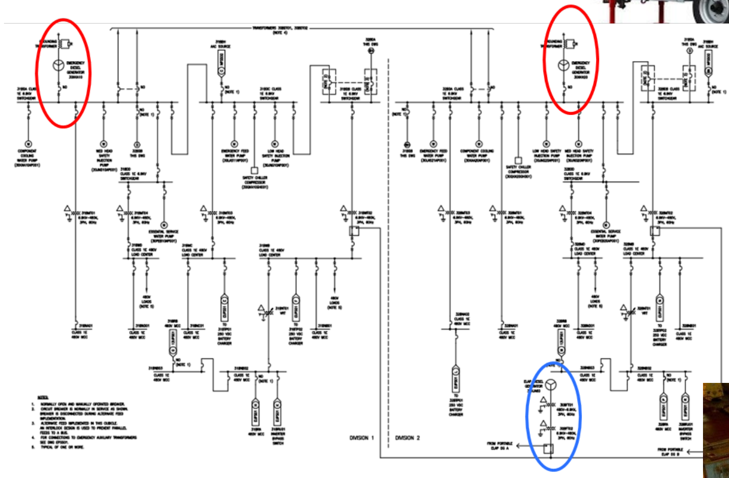
- Reinforced capabilities for heat transfer to the UHS. Alternative heat sink or different access is required if heat transfer cannot be ensured in conditions generated by hazards more severe than those selected for the design basis



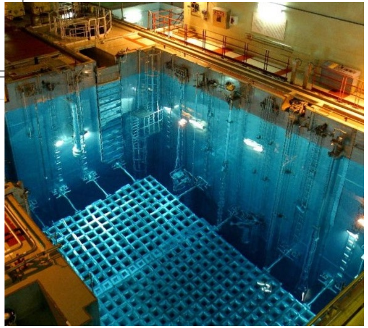
UHS=Ultimate Heat Sink

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)

IAEA Safety Standards
for protecting people and the environment

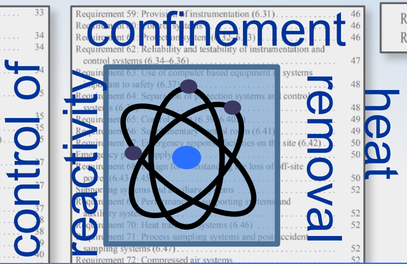
Safety of
Nuclear Power Plants:
Design

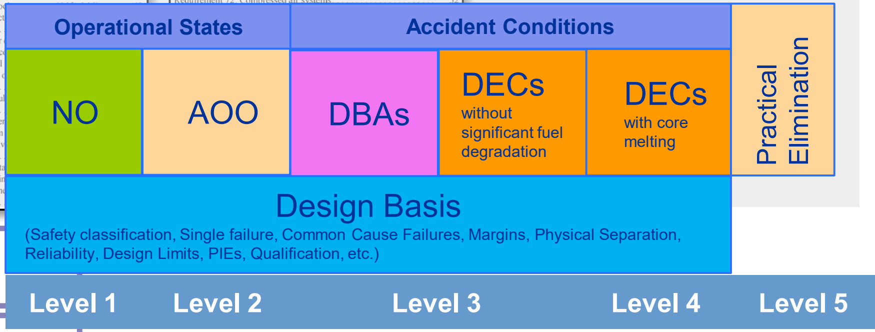
Specific Safety Requirements
No. SSR-2/1 (Rev. 1)

IAEA
International Atomic Energy Agency

SSR 2/1 (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

+Concept of Practical Elimination

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.

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.

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 4: Fundamental safety functions (FSFs)

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

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

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

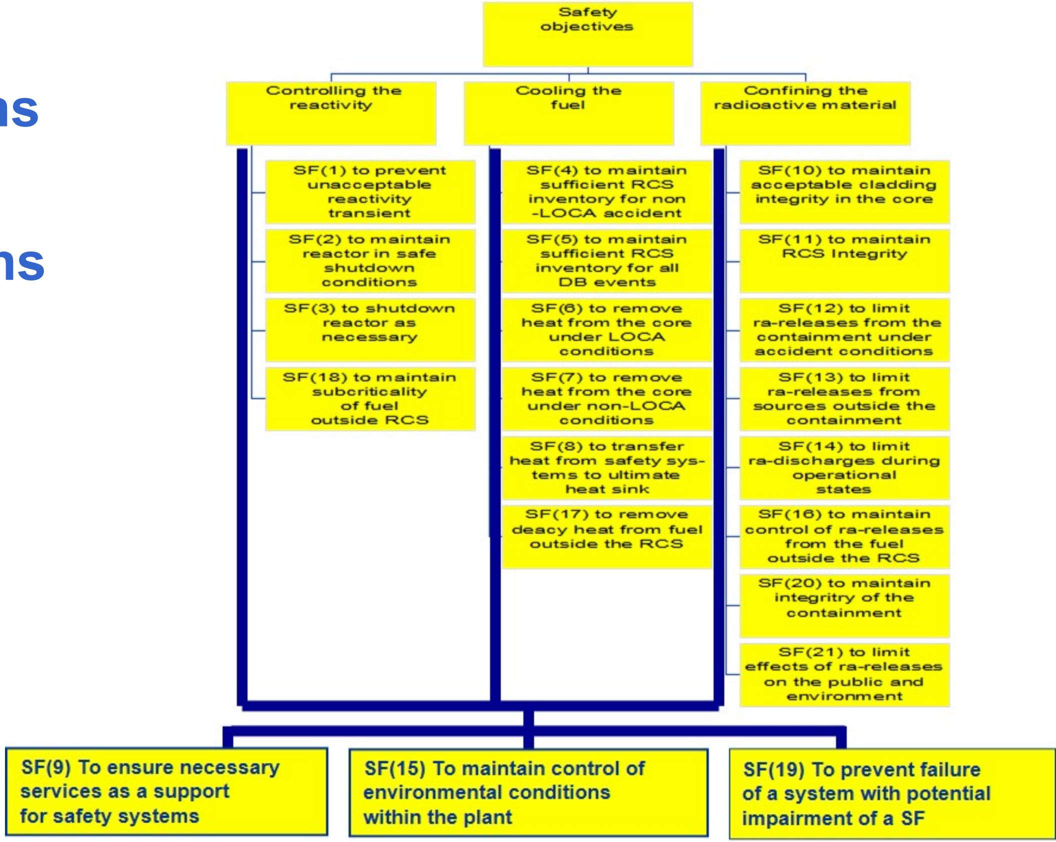
Means of monitoring the status of the plant shall be provided for ensuring that the required safety functions are fulfilled.

Fundamental and subordinated safety functions. Examples

IAEA

Fundamental safety functions

Subordinated safety functions applicable for LWRs



Principal Technical Requirements

Requirement 5: Radiation protection

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

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

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

Principal Technical Requirements

Requirement 6: Design for a nuclear power plant

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

Principal Technical Requirements

Requirement 7: Application of defence in depth

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

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

Principal Technical Requirements

Requirement 7: Application of defence in depth

…

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

Principal Technical Requirements

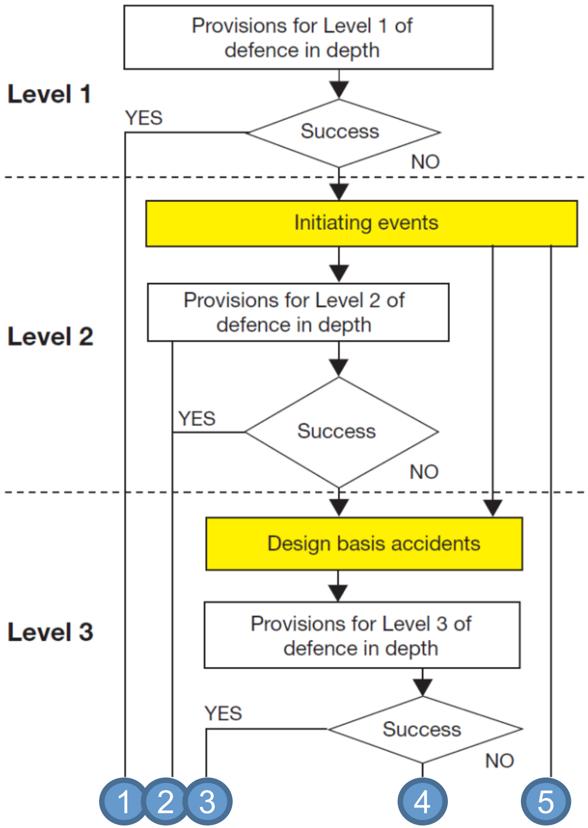
Requirement 7: Application of defence in depth (cont.)

…

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

- The levels of defence in depth shall be <u>independent</u> as far as practicable to avoid a failure of one level reducing the effectiveness of other levels. In particular, <u>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</u>.

Defence in Depth objectives



Objective:
Prevention of abnormal operation and failures

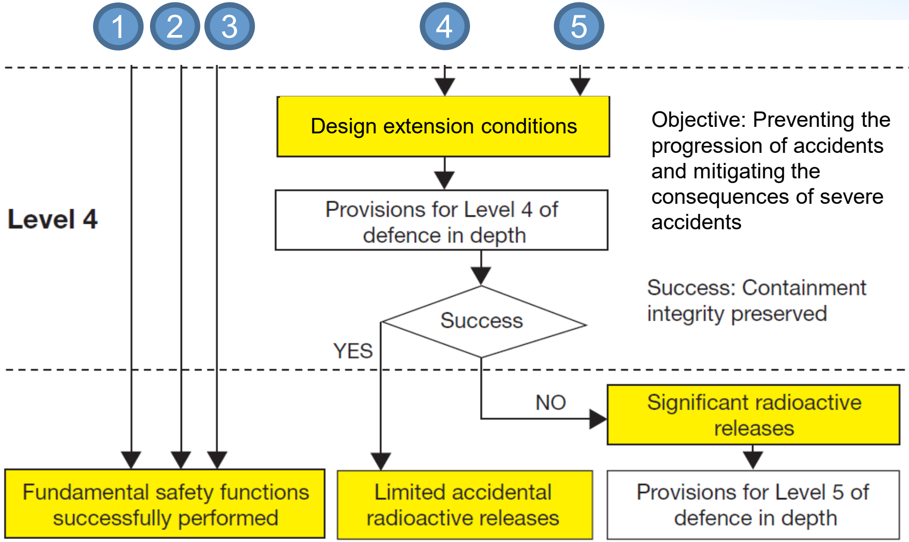
Success:
Normal operation

Objective: Control of abnormal operation and detection of failures

Success: Return to normal operation after recovery from failure. Prevention of progress of AOOs

Objective:
Control of accidents (below the severity level postulated within the design basis)

Success: Accident consequences limited within the design basis



Objective: Preventing the progression of accidents and mitigating the consequences of severe accidents

Success: Containment integrity preserved

Defence in Depth ↔ Plant design basis

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	Robust design and high quality in construction of normal operation systems, including monitoring and control systems	Operational limits and conditions 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 and/or emergency operating procedures	Level 2
Level 3 3a	Control of design basis accidents	Safety systems	Emergency operating procedures	Level 3
Level 3 3b	Control of design extension conditions to prevent core melting	Safety features for design extension conditions without significant fuel degradation	Emergency operating procedures	Level 4
Level 4	Control of design extension conditions to mitigate the consequences of severe accidents	Safety features for design extension conditions with core melting. Technical support centre	Severe accident management guidelines	
Level 5	Mitigation of the radiological consequences of significant releases of radioactive substances	On-site and off-site emergency response facilities	On-site and off-site emergency plans and procedures	Level 5

Table from SSG-88

Defence in Depth ↔ Plant design basis

Approach 1, acceptable limits on predicted radiological consequences for design extension conditions without significant fuel degradation may be the same as, or similar to, acceptable limits for design basis accidents. Furthermore, the physical phenomena associated with design basis accidents and design extension conditions without significant fuel degradation are similar, although there might be differences in the analysis. In contrast, the physical phenomena associated with design extension conditions with core melt are completely different.

Defence in Depth ↔ Plant design basis

Approach 2, design extension conditions without significant fuel degradation and design extension conditions with core melt are considered together in the fourth level of defence in depth. This approach emphasizes the distinction between the set of rules to be applied for design extension conditions and the set of rules to be applied for design basis accidents, both in the design and in the safety assessment.

Despite their differences, both approaches are in compliance with para. 5.29(a) of SSR-2/1 (Rev. 1) [1] and support the implementation, to the extent practicable, of independence between safety systems and those safety features for design extension conditions.

Principal Technical Requirements

Requirement 8: Interfaces of safety with security and safeguards

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

Principal Technical 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 for a nuclear power plant shall preferably be of a **design that has previously been proven** in equivalent applications, and if not, shall be items of high quality and of a technology that has been qualified and tested.
- National and international codes and standards that are used as design rules for items important to safety shall be identified and evaluated to determine their applicability, adequacy and sufficiency
- **Where an unproven design or feature is introduced** or where 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** or the examination of operating experience from other relevant applications. The new design or feature or new practice shall also be adequately tested to the extent practicable before being brought into service, and shall be monitored in service to verify that the behaviour of the plant is as expected.

Principal Technical Requirements

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.**

Principal Technical Requirements

Requirement 11: Provision for construction

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

Requirement 12: Features to facilitate radioactive waste management and decommissioning

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

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.

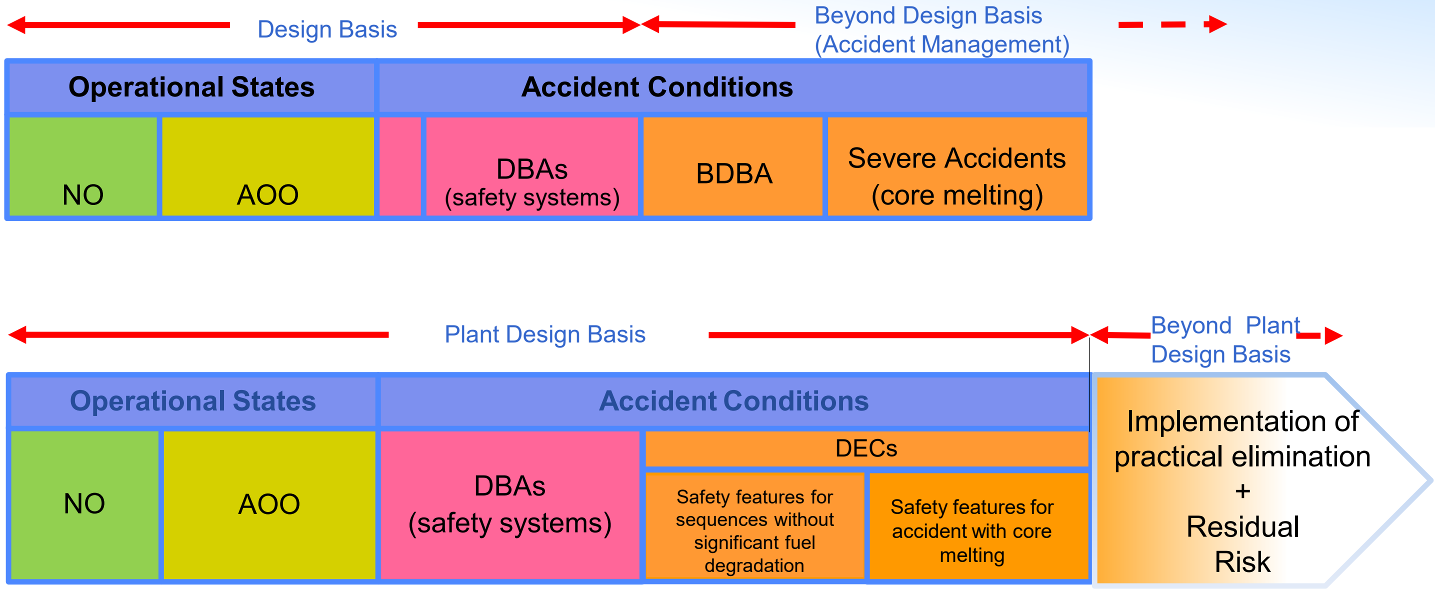
Design Extension Conditions (DECs). IAEA Definition:

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

Earlier Concept

SSR-2/1, 2012



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*.

Design Basis

Requirement 14: Design basis for items important to safety

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

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

Plant Design Basis - Plant Design Envelope

"**Design Basis of the plant**" is a common, not very precise and, in some cases, a misleading term. It refers to the range of conditions and events taken explicitly into account in the design of a facility, according to established criteria, such that the facility can withstand them without exceeding authorized limits by the planned operation of safety systems (features)

Saying, that a specific accident is included in the **design basis of the plant** (e.g. it is a design basis accident) means in reality that the conditions generated by this 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.

However, each plant SSC to be correctly designed needs its own specific design basis

The introduction of equipment designed for DEC, suggests that the design basis of the plant is extended. To avoid controversy with national regulations that don't consider equipment for DEc within the "plant design basis" the term **"Plant design envelope**" to denote the range of conditions (including DEC) for which the plant is designed

Design Basis for SSCs

Design Basis (SSR 2/1) : Set of information which identifies for each SSC conditions, needs and requirements necessary for its design :

- the functions to be performed by the SSC of a facility
- the operational states, accident conditions in which it is required
- conditions generated by internal and external hazards that the structure, system and component has to withstand
- the acceptance criteria for the necessary capability, reliability, availability and functionality

Plant Sates & Design Basis

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

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

<table>
<tr><th colspan="5">Plant design envelope</th></tr>
<tr><th colspan="2">Operational states</th><th colspan="3">Accident conditions</th></tr>
<tr><td>NO</td><td>AOO</td><td>DBAs</td><td colspan="2">Design Extension Conditions</td></tr>
<tr><td colspan="3"></td><td>Without significant fuel degradation</td><td>With core melting (severe accidents)</td></tr>
<tr><td colspan="5">Loads and conditions generated by External & Internal Hazards (for each plant state)</td></tr>
<tr><td colspan="5">Criteria for functionality, capability, margins, layout and reliability (for each plant state)</td></tr>
<tr><td colspan="2" rowspan="2">Design basis of equipment for Operational states</td><td rowspan="2">Design Basis of Safety Systems
including SSCs necessary to control DBAs and some AOOs</td><td colspan="2">Design Basis of safety features for DECs
including SSCs necessary to control DECs</td></tr>
<tr><td>Features to prevent core melt</td><td>Features to mitigate core melt
(Containment systems)</td></tr>
</table>

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

Design Basis

Requirement 15: Design limits

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

- The design limits shall be specified and shall be consistent with relevant national and international standards and codes, as well as with relevant regulatory requirements.

Design Basis

Requirement 16: Postulated initiating events

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

The postulated initiating events shall be identified on the basis of engineering judgement and a combination of deterministic assessment and probabilistic assessment.

The postulated initiating events shall include all foreseeable failures of structures, systems and components of the plant, as well as operating errors and possible failures arising from internal and external hazards

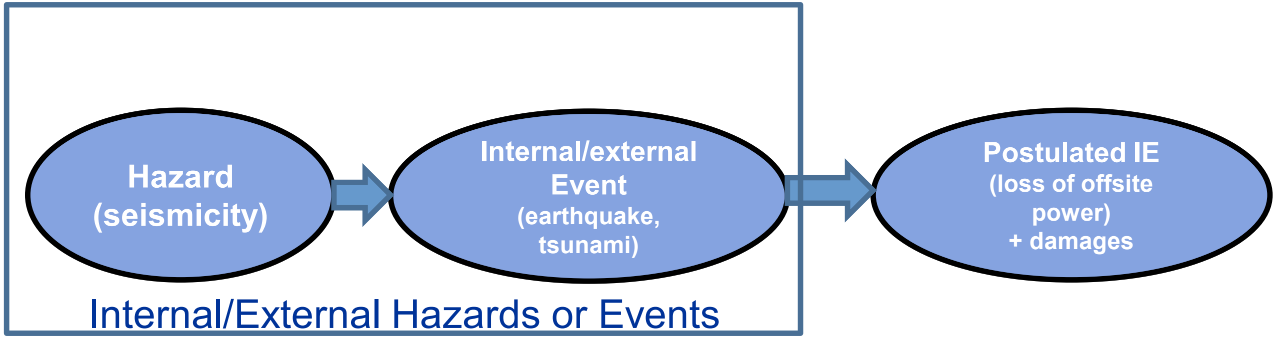
The expected plant response to any postulated initiating event shall be such that the following can reasonably be achieved, in order of preference by : inherent plant characteristics, passive safety features or by the action of systems in operation, safety systems, specified procedural actions.

Internal and External Hazards

The hazard describes the circumstances that may lead to an event, e.g. the presence of combustible material may lead to a fire. However, in this context, the words hazard and event are used often as synonymous in IAEA SSs and other IAEA publications

Internal and external hazards have the potential to induce an initiating event and to cause damage to several or many plant equipment or affect plant operation (and even outside emergency response)

The Internal or the External Hazard is not an initiating event



Design Basis

Requirement 17: Internal and external hazards

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

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

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

Design Basis

Requirement 18: Engineering design rules

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

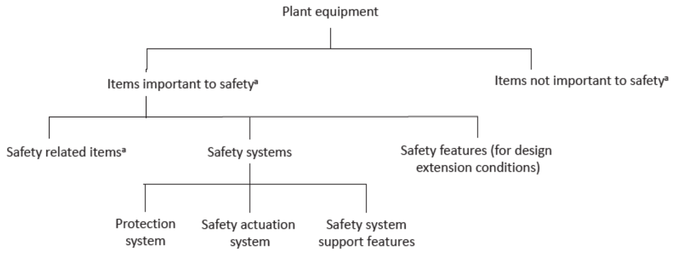
Design Basis

Requirement 19: Design basis accidents

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

- DBAs are used to define the design basis of the “safety systems” and for other items important to safety that are necessary to control those accidents
- Safety systems are designed with the application of the “single failure criterion”
- Key plant parameters shall not exceed specified design limits. No or only minor radiological impacts, both on and off the site, and do not necessitate any off-site intervention measures
- Design Basis Accidents shall be analysed in a conservative manner.

plant equipment (for a nuclear power plant)



[a] In this context, an ‘item’ is a structure, system or component.

Design Basis

IAEA

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.

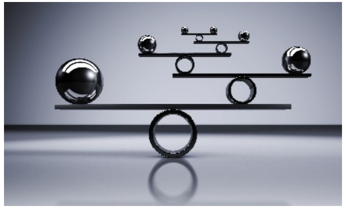
Design Basis

Requirement 21: Physical separation and independence of safety systems

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

Requirement 22: Safety classification

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



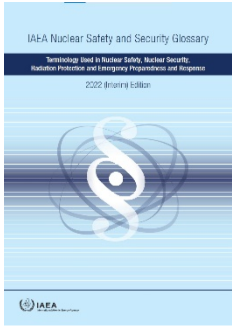
The method for classifying the safety significance of items important to safety shall be based primarily on deterministic methods complemented, where appropriate, by probabilistic methods, with due account taken of factors such as: the safety function(s) to be performed by the item; the consequences of failure to perform a safety function; the frequency with which the item will be called upon to perform a safety function, etc.

Plant equipment categories

plant equipment (for a nuclear power plant)

- Plant equipment
  - Items important to safety[a]
    - Safety related items[a]
    - Safety systems
      - Protection system
      - Safety actuation system
      - Safety system support features
    - Safety features (for design extension conditions)
  - Items not important to safety[a]

[a] In this context, an 'item' is a structure, system or component.



Design Basis

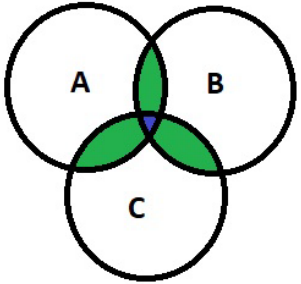
Requirement 23: Reliability of items important to safety

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

VS

Requirement 24: Common cause failures

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



Requirement 25: Single failure criterion

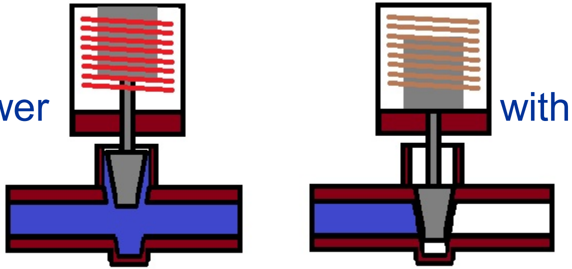
The single failure criterion shall be applied to each safety group incorporated in the plant design.

Design Basis

Requirement 26: Fail-safe design

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

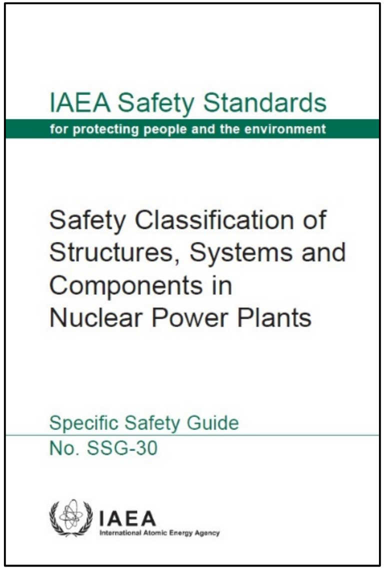
with electric power



without electric power

Requirement 27: Support service systems

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


IAEA Safety Standards
for protecting people and the environment

Safety Classification of Structures, Systems and Components in Nuclear Power Plants

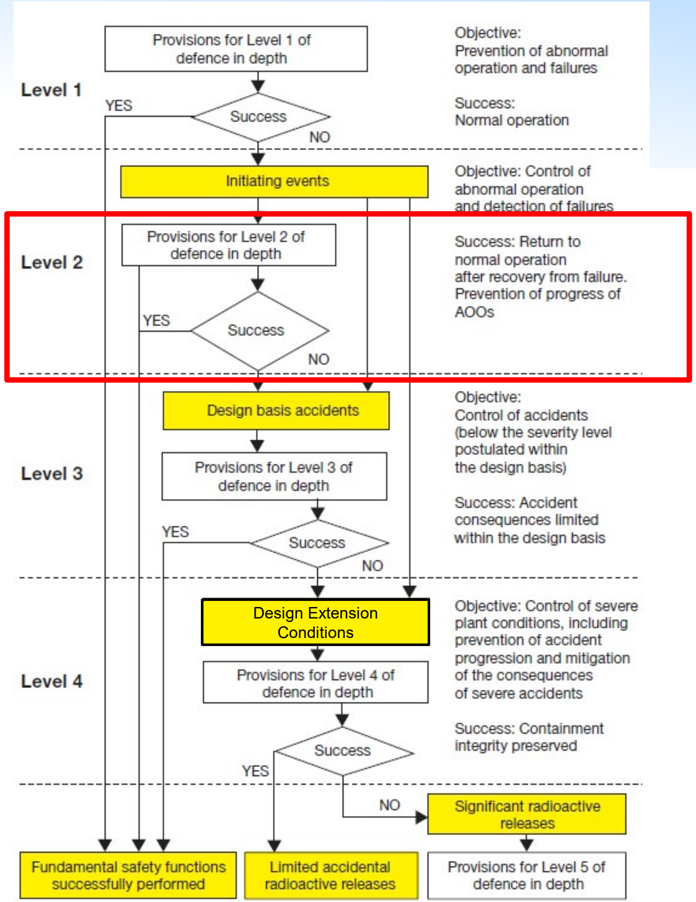
Specific Safety Guide
No. SSG-30

IAEA
International Atomic Energy Agency

Design Basis

Requirement 28: Operational limits and conditions for safe operation

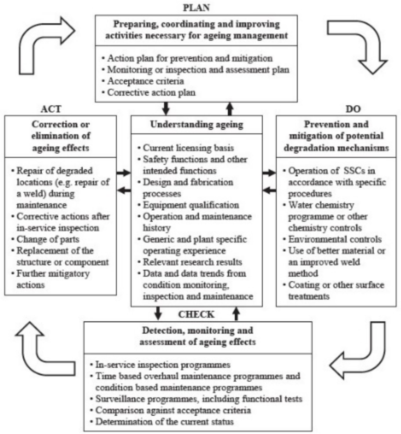
The design shall establish a set of operational limits and conditions for safe operation of the nuclear power plant.



Design for safe operation over the lifetime of the plant

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

Requirement 30: Qualification of items important to safety



Requirement 31: Ageing management

Human factors

Requirement 32: Design for optimal operator performance

Main control room of experimental High Temperature Gas cooled Reactor at Tshinghua University, Beijing, China,.

Main control room at the Madras NPP, Kalpakkam, India.

Main control room of the Qinshan NPP, Phase 1, China.

Other design considerations

Requirement 33: Safety systems, and safety features for design extension conditions, of units of a multiple unit nuclear power plant

Requirement 34: Systems containing fissile material or radioactive material

Requirement 35: Nuclear power plants used for cogeneration of heat and power, heat generation or desalination

Wolsong NPP, Republic of Korea

Eurodif & Tricastin NPP, France

Other design considerations

Requirement 36: Escape routes from the plant

Requirement 37: Communication systems at the plant

Requirement 38: Control of access to the plant

Requirement 39: Prevention of unauthorized access to, or interference with, items important to safety

Access route to Temelin NPP, Czech Republic

Access control at Temelin NPP, Czech Republic

Other design considerations

Requirement 40: Prevention of harmful interactions of systems important to safety

Requirement 41: Interactions between the electrical power grid and the plant

Paluel NPP, France

Embalse NPP, Argentina

Safety Analysis

IAEA

Requirement 42: Safety analysis of the plant design

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

- On the basis of a safety analysis, the design basis for items important to safety and their links to initiating events and event sequences shall be confirmed. It shall be demonstrated that the nuclear power plant as designed is capable of complying with authorized limits on discharges with regard to radioactive releases and with the dose limits in all operational states, and is capable of meeting acceptable limits for accident conditions.
- The safety analysis shall provide assurance that defence in depth has been implemented in the design of the plant.
- The safety analysis shall provide assurance that uncertainties have been given adequate consideration in the design of the plant and in particular that adequate margins are available to **avoid cliff edge effects** and early radioactive releases or large radioactive releases.
- The applicability of the analytical assumptions, methods and degree of conservatism used in the design of the plant shall be updated and verified for the current or as built design.

Design safety

Specific Plant System Requirements

Design of specific plant systems

	Requirement #
Reactor core and associated features	**(R43-R46)**
Reactor coolant system	**(R47-R53)**
Containment structure and containment system	**(R54-R58)**
Instrumentation and control systems	**(R59-R67)**
Emergency power supply	**(R68)**
Supporting systems and auxiliary systems	**(R69-R76)**
Other power conversion systems	**(R77)**
Treatment of radioactive effluents and radioactive waste	**(R78-R79)**
Fuel handling and storage systems	**(R80)**
Radiation protection	**(R81-R82)**

Conclusion

IAEA

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

How to contact us

Safety.Standards@iaea.org

IAEA
International Atomic Energy Agency
Atoms for Peace and Development

Thank you!