International Atomic Energy Agency

# Safety of Nuclear Power Plants: Design
# SSR 2/1

Joint ICTP-IAEA Essential Knowledge Workshop on Deterministic Safety Analysis and Engineering Aspects Important to Safety

Trieste, 12-23 October 2015

***J. Yllera***

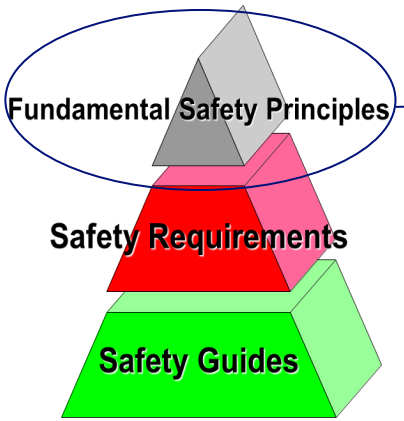
IAEA, Division of Nuclear Installation Safety

# Objectives and Outline

**The presentation is aimed at understanding the most relevant aspects of the new IAEA Safety Requirements for the Design of Nuclear Power Plants, including:**

- **Safety principles and concepts, e.g. Defence in Depth and its implementation in the design**
- **Principal Technical Requirements**
- **General Plant Design Requirements**
- **System Specific Safety Requirements**

# IAEA Fundamental Safety Principles (2006)



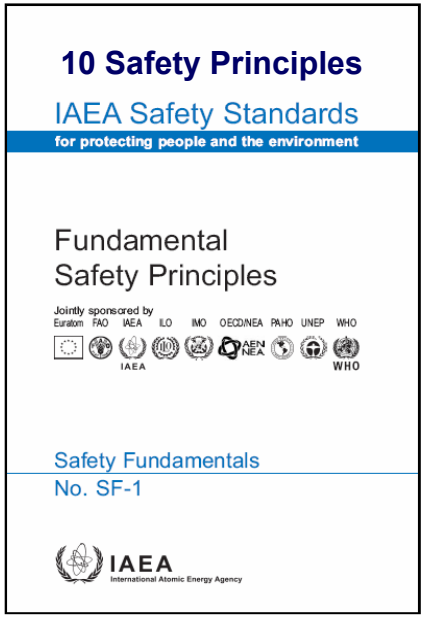

## Safety Objective

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

**Responsibility for Safety**

**Role of Government**

**Leadership and Management for Safety**




**Protective Actions to Reduce Existing Or Unregulated Radiation Risks**

**Emergency Preparedness and Response**

**Prevention of Accidents**

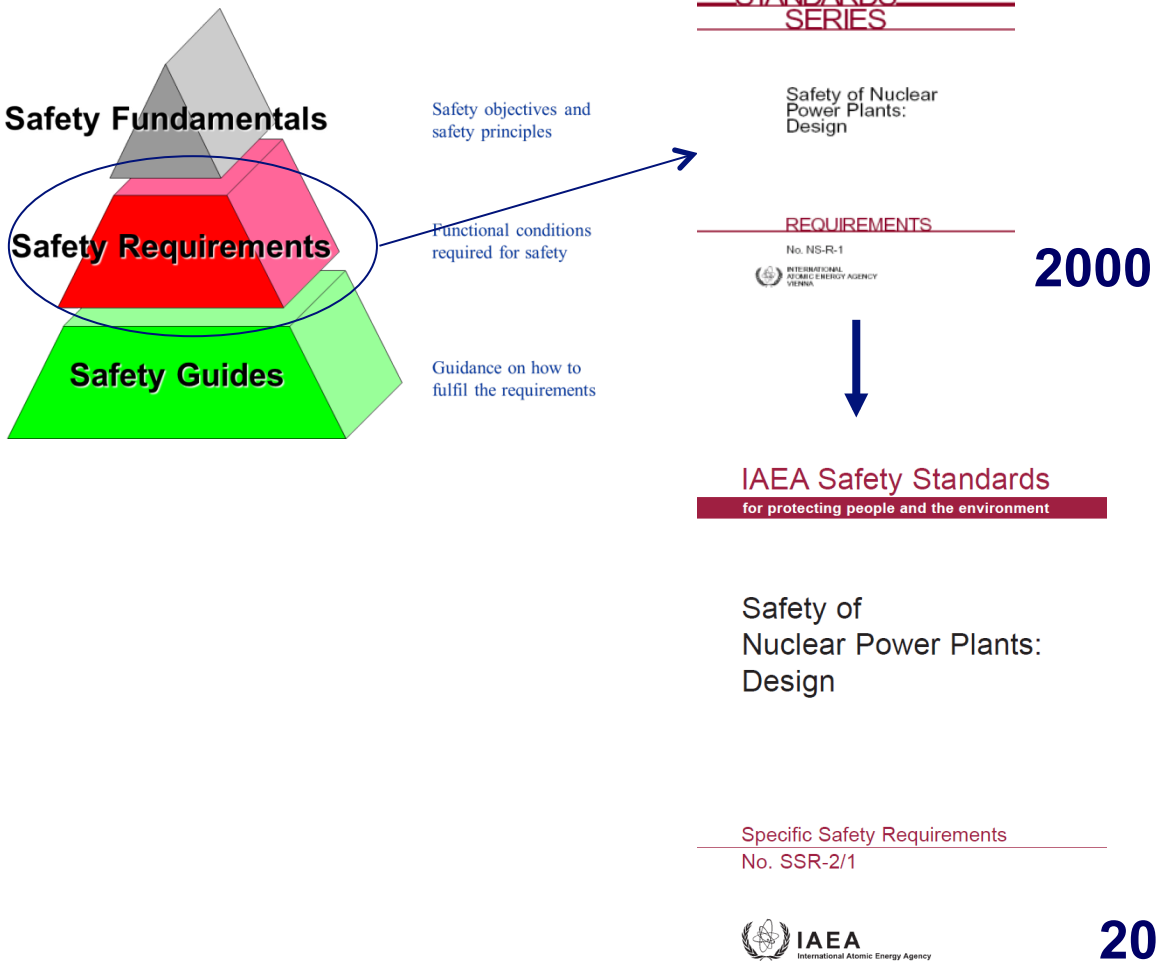
**Justification of Facilities and Activities**

**Optimization of Protection**

**Limitation of Risks to Individuals**

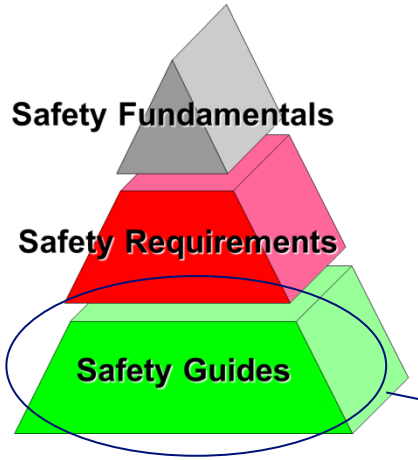
**Protection of Present and Future Generations**

# Requirements for Design of NPPs




- To be implemented by the designer to fulfill the fundamental safety functions with the appropriate level of defence in depth
- To be used by the reviewer of the design (e.g. Safety Authority) to assess the safety of the design

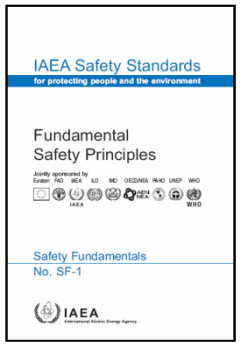
# IAEA Safety Standards for Design of NPPs

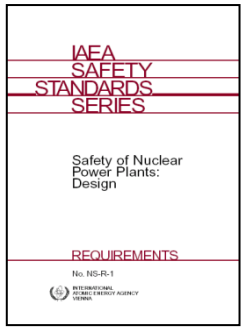



Safety objectives and safety principles

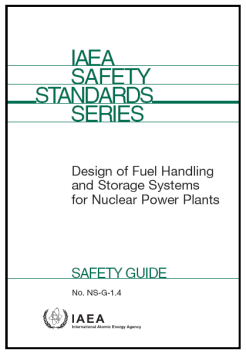
Functional conditions required for safety

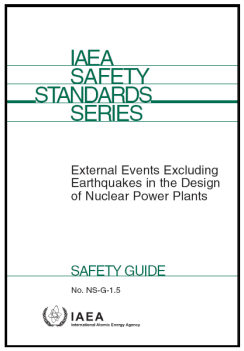
Guidance on how to fulfil the requirements

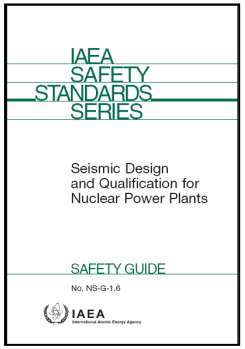


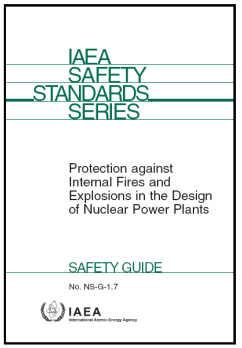



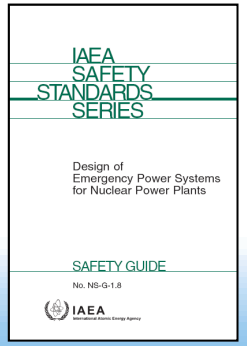


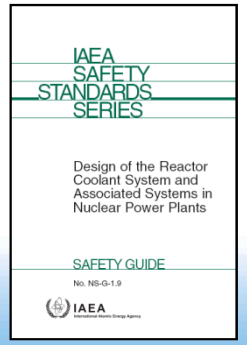



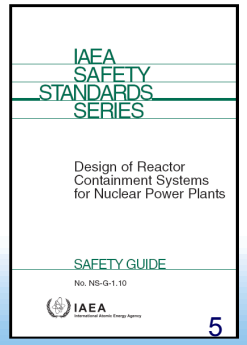



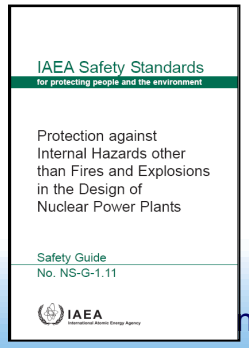



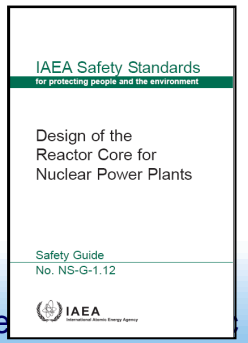



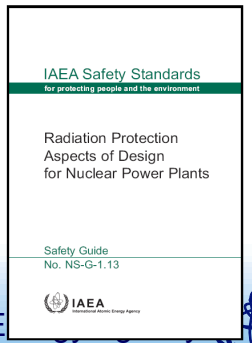



# SSR 2/1 - Applicability

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

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

# Importance of the Requirements for the Design of NPPs

- Define the safety approach and establish the safety “level” for designs of nuclear power plants
  - reflect the state of the art
  - reflect the views and the licensing practices of the majority of IAEA Member States
  - document of large consensus

- provide the links with the requirements for site evaluation and for operation
  - taking into consideration the impact of the site on the design
  - providing for easy and safe operation

# Importance of the Requirements for the Design of NPPs

- are the main reference to perform design safety reviews
  - basis for the preparation of guidelines to conduct design safety review
- 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

# Structure of SSR 2/1

- **Sections 1-2 : Introduction, Principles and Concepts**
- **Section 3 : Requirements on Management of Safety in design**
- **Sections 4- 5 : Requirements applicable to all SSCs important to safety**
- **Section 6: Requirements for specific plant systems, e.g.:**

  **Reactor core, Reactor coolant systems, Containment systems, I&C, Emergency power supply, Radioactive effluents treatment, Fuel handling and storage systems**

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

- INTRODUCTION
- APPLYING SAFETY PRINCIPLES AND CONCEPTS

Safety objectives; Radiation protection; Defence in depth

- MANAGEMENT OF SAFETY IN DESIGN
  - 3 Requirements
- PRINCIPAL TECHNICAL REQUIREMENTS
  - 9 Requirements
- GENERAL PLANT DESIGN
  - Design Basis (16 Requirements)
  - Safe Operation Over Lifetime of Plant (3 Requirements)
  - Human Factors (1 Requirement)
  - Other Design Considerations (9 Requirements)
  - Safety Analysis (1 Requirement)
- DESIGN OF SPECIFIC PLANT SYSTEMS
  - Reactor Core and Associated Features (4 Requirements)
  - Reactor Coolant Systems (7 Requirements)
  - Containment Structure and Containment System (5 Requirements)
  - Instrumentation and Control Systems (9 Requirements)
  - Emergency Power Supply (1 Requirement)
  - Supporting Systems and Auxiliary Systems (8 Requirements)
  - Other Power Conversion Systems (1 Requirement)
  - Treatment of Radiological Effluents and Radioactive Waste (2 Requirements)
  - Fuel Handling and Storage System (1 Requirement)
  - Radiation Protection (2 Requirements)

**82 REQUIREMENTS ("SHALL" STATEMENTS)**

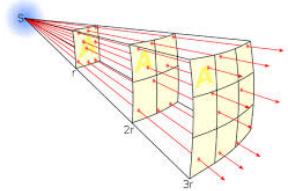
# Introduction, Principles and Concepts

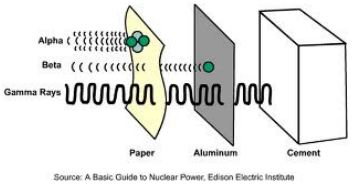
# The FSP 8, "Prevention of Accidents", indicates that:

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

- The primary means of preventing and mitigating the consequences of accidents is "**defence in depth (DiD)**"
- DiD is implemented through the combination of a number of consecutive and independent levels of protection.

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






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

# MANAGEMENT OF SAFETY IN DESIGN

## SSR 2/1 REQUIREMENTS 1 THROUGH 3

# Management of Safety in Design

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

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

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

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

# Management of Safety in Design

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

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

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

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

# PRINCIPAL TECHNICAL REQUIREMENTS
## SSR 2/1 REQUIREMENTS 4 THROUGH 12

# 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 <u>all plant states</u>**

  - 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.

# Principal Technical Requirements

- **Requirement 5: Radiation protection**

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

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

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

# Principal Technical Requirements

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

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

  - The design shall **meet the requirements** of the owner and the operating organization, the requirements of the regulatory body and the requirements of relevant legislation, and relevant and applicable national and international codes and standards
  - due **account is taken of human capabilities** and limitations and factors that could influence human performance
  - due **account of relevant available experience** that has been gained in the design, construction and operation of other plants and of the results of relevant research programmes.
  - due **account of the results of deterministic and probabilistic safety analyses**, and an iterative process shall be carried out by means of which it shall be ensured that due consideration has been given to the prevention of accidents and the mitigation of their consequences.
  - the generation of radioactive **waste and radioactive discharges** are kept **as low as reasonably achievable**

# Principal Technical Requirements

- **Requirement 7: Application of defence in depth**
  **The design of a nuclear power plant shall incorporate defence in depth. The levels of defence in depth shall be independent as far as is practicable**.

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

  - Relaxations shall be justified for specific modes of operation

# Principal Technical Requirements

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

  ...

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

# Principal Technical Requirements

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

  ...

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

# Principal Technical Requirements

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

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

- **Requirement 9: Proven engineering practices**

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

# Principal Technical Requirements

- **Requirement 10: Safety assessment**

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

- **Requirement 11: Provision for construction**

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

# Principal Technical Requirements

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

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

# GENERAL PLANT DESIGN

## SSR 2/1 REQUIREMENTS 13 THROUGH 42

# General Plant Design

- **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 |

# General Plant Design – Design Basis

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

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

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

- **Requirement 15: Design limits**

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

  Design limits shall be consistent with regulations and standards

# General Plant Design – 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.

# General Plant Design – 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.

# General Plant Design – Design Basis

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

…

***External hazards***

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

# General Plant Design – 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.**

- **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.

# General Plant Design - Design Basis

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

## 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

# General Plant Design - Design Basis

**Safety features for DEC:**

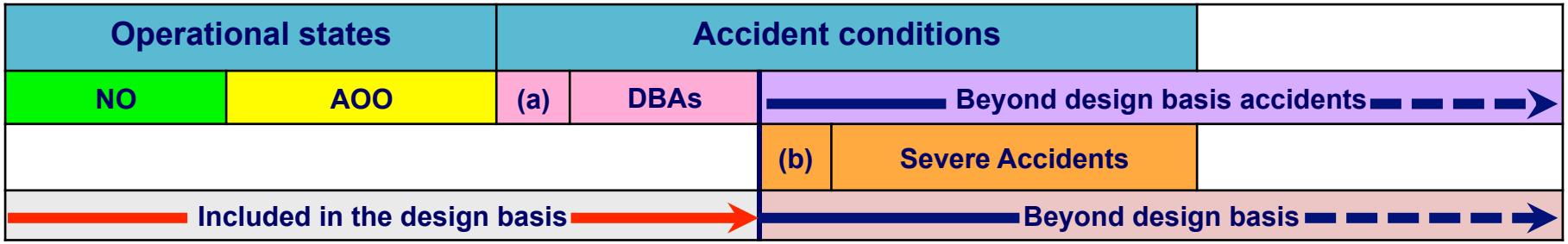
- Shall be independent, to the extent practicable, of those used in more frequent accidents;
- Shall be capable of performing in the environmental conditions related to DEC, including severe accidents, where appropriate;
- In particular, the containment and its safety features shall be able to withstand 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 DEC 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.

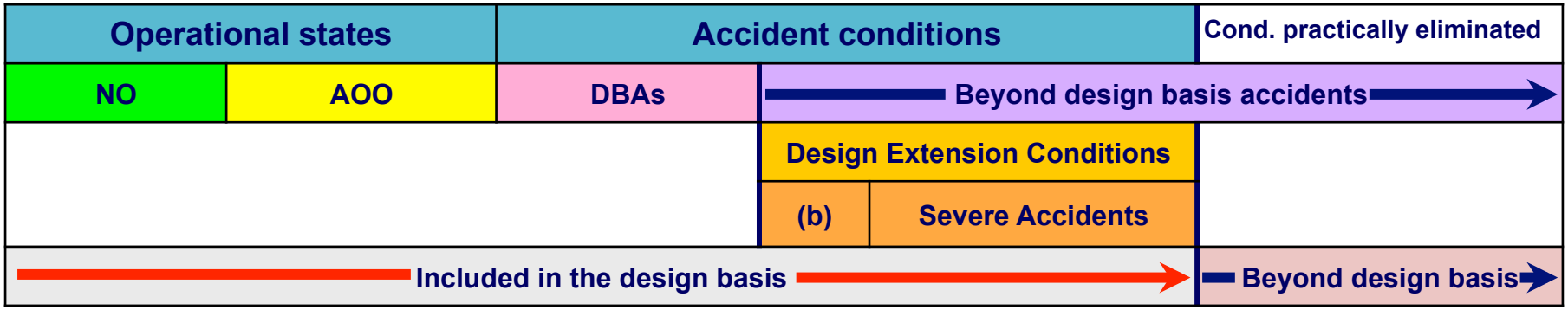
(*) The possibility of certain conditions occurring is considered to have been practically eliminated if it is physically impossible for the conditions to occur or if the conditions can be considered with a high degree of confidence to be extremely unlikely to arise.

# SSR 2/1 versus NS-R-1, plant states

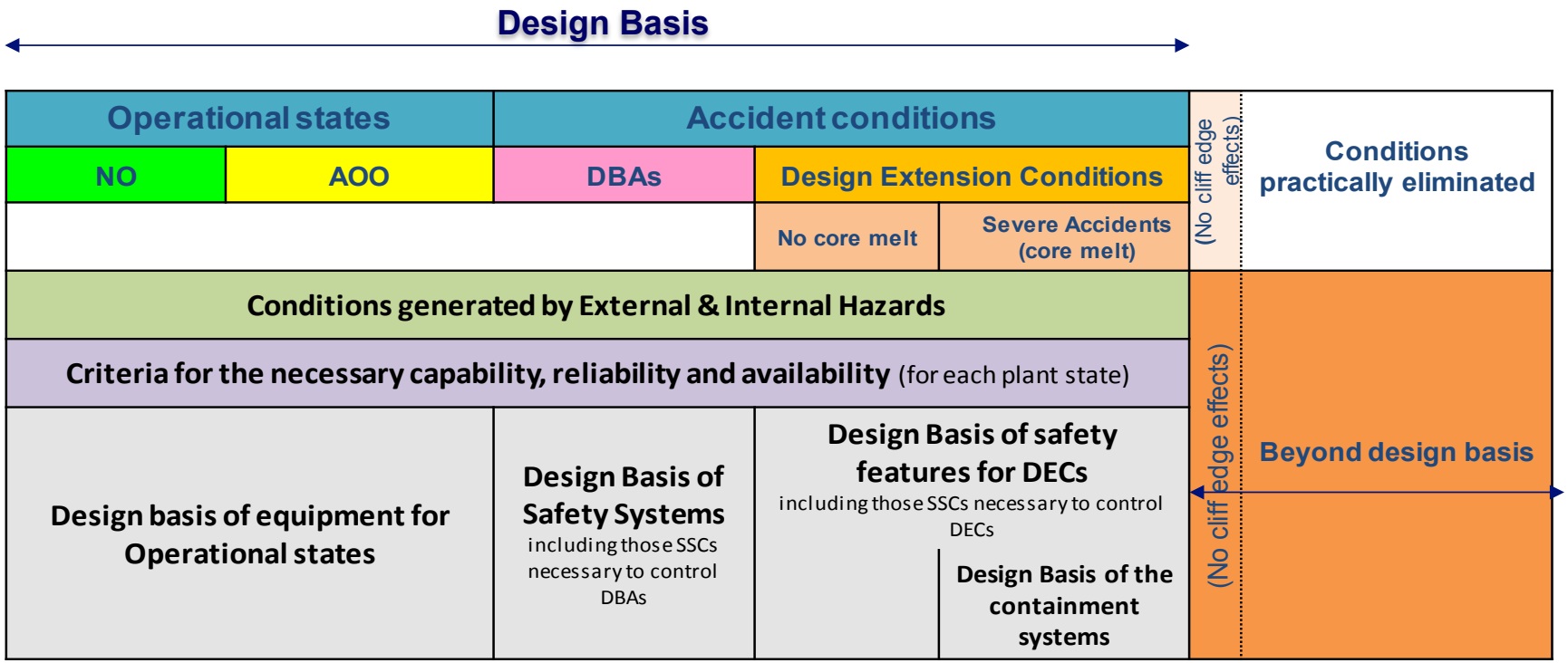
## NS-R-1, 2000




## SSR-2/1, 2012



# Plant Sates & Design Basis




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

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

# General Plant Design - Design Basis

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

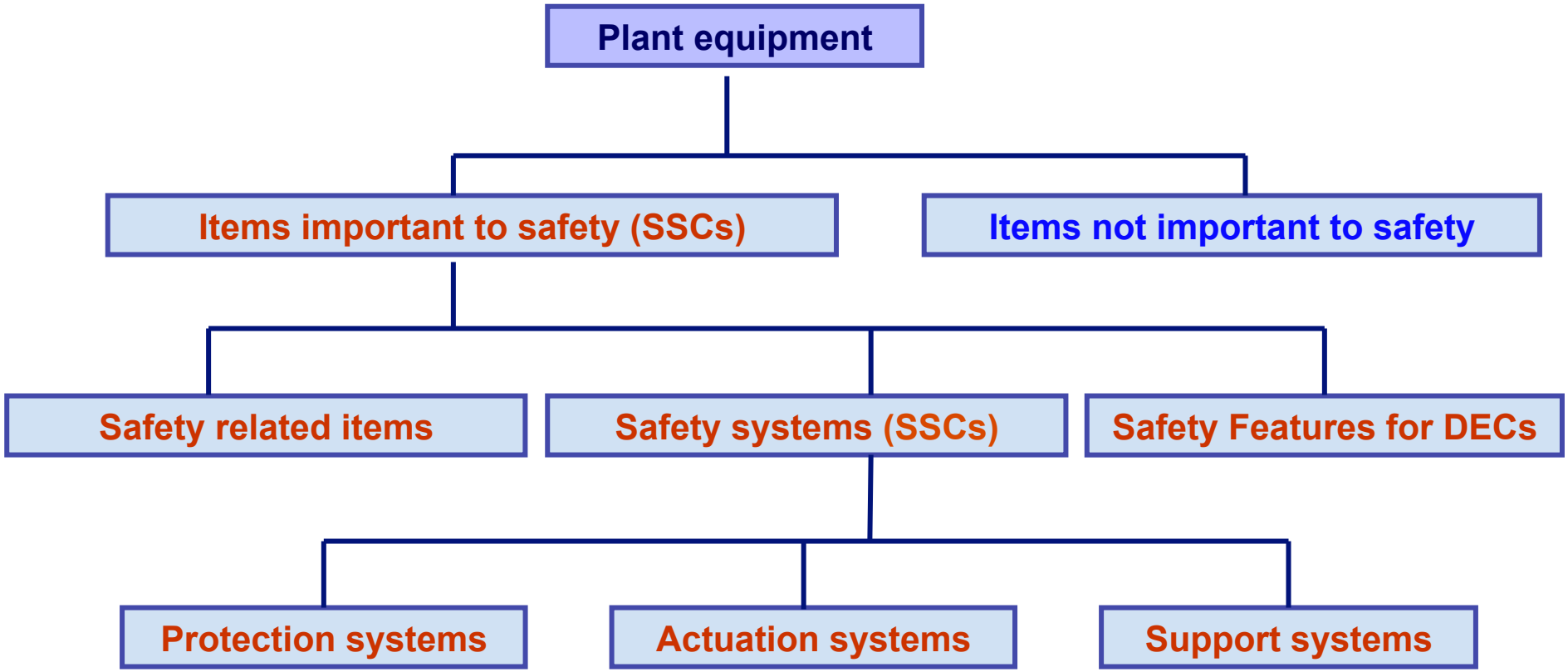
**Interference between safety systems or between redundant elements of a system shall be prevented by means such as physical separation, electrical isolation, functional independence and independence of communication (data transfer), as appropriate.**

- **Requirement 22: Safety classification**

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

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

# Plant Equipment Categories




* SSCs = Systems, structures and components

# General Plant Design - Design Basis

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

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

- **Requirement 24: Common cause failures**

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

- **Requirement 25: Single failure criterion**

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

# General Plant Design - Design Basis

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

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

- **Requirement 27: Support service systems**

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

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

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

# General Plant Design

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

- **Requirement 30: Qualification of items important to safety**
  - A qualification programme for items important to safety shall be implemented to verify that items important to safety at a nuclear power plant are capable of performing their intended functions when necessary, and in the prevailing environmental conditions, throughout their design life, with due account taken of plant conditions during maintenance and testing.

# General Plant Design

DESIGN FOR SAFE OPERATION OVER THE LIFETIME OF THE PLANT

- **Requirement 31: Ageing management**

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

# General Plant Design
# Human Factors

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

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

# General Plant Design

## OTHER DESIGN CONSIDERATIONS

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

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

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

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

# General Plant Design

## OTHER DESIGN CONSIDERATIONS

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

  Nuclear power plants coupled with heat utilization units (such as for district heating) and/or water desalination units shall be designed to prevent processes that transport radionuclides from the nuclear plant to the desalination unit or the district heating unit under conditions of operational states and in accident conditions.

- **Requirement 36: Escape routes from the plant**

  A nuclear power plant shall be provided with a sufficient number of escape routes, clearly and durably marked, with reliable emergency lighting, ventilation and other services essential to the safe use of these escape routes.

# General Plant Design

## OTHER DESIGN CONSIDERATIONS

- **Requirement 37: Communication systems at the plant**

  Effective means of communication shall be provided throughout the nuclear power plant to facilitate safe operation in all modes of normal operation and to be available for use following all postulated initiating events and in accident conditions.

- **Requirement 38: Control of access to the plant**

  The nuclear power plant shall be isolated from its surroundings with a suitable layout of the various structural elements so that access to it can be controlled.

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

  Unauthorized access to, or interference with, items important to safety, including computer hardware and software, shall be prevented.

# General Plant Design

## OTHER DESIGN CONSIDERATIONS

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

  The potential for harmful interactions of systems important to safety at the nuclear power plant that might be required to operate simultaneously shall be evaluated, and effects of any harmful interactions shall be prevented.

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

  The functionality of items important to safety at the nuclear power plant shall not be compromised by disturbances in the electrical power grid, including anticipated variations in the voltage and frequency of the grid supply.

# General Plant Design

## SAFETY ANALYSIS

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

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

  - Deterministic approach
  - Probabilistic approach

# DESIGN OF SPECIFIC PLANT SYSTEMS

## SSR 2/1 REQUIREMENTS 43 THROUGH 82

# Design of Specific Plant Systems

## REACTOR CORE AND ASSOCIATED FEATURES

- **Requirement 43: Performance of fuel elements and assemblies**
  - Fuel elements and assemblies for the nuclear power plant shall be designed to maintain their structural integrity, and to withstand satisfactorily the anticipated radiation levels and other conditions in the reactor core, in combination with all processes of deterioration that could occur in operational states.

- **Requirement 44: Structural capability of the reactor core**
  - The fuel elements and fuel assemblies and their supporting structures for the nuclear power plant shall be designed so that, in operational states and in accident conditions other than severe accidents, a geometry that allows for adequate cooling is maintained and the insertion of control rods is not impeded.

# Design of Specific Plant Systems

## REACTOR CORE AND ASSOCIATED FEATURES

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

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

- **Requirement 46: Reactor shutdown**

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

  - The means for shutting down the reactor shall consist of at least two diverse and independent systems.
  - At least one of the two different shutdown systems shall be capable, on its own, of maintaining the reactor subcritical by an adequate margin and with high reliability, even for the most reactive conditions of the reactor core.

# Design of Specific Plant Systems

## REACTOR COOLANT SYSTEMS

- **Requirement 47: Design of reactor coolant systems**
  - The components of the reactor coolant systems for the nuclear power plant shall be designed and constructed so that the risk of faults due to inadequate quality of materials, inadequate design standards, insufficient capability for inspection or inadequate quality of manufacture is minimized.
- **Requirement 48: Overpressure protection of the reactor coolant pressure boundary**
  - Provision shall be made to ensure that the operation of pressure relief devices will protect the pressure boundary of the reactor coolant systems against overpressure and will not lead to the release of radioactive material from the nuclear power plant directly to the environment.

# Design of Specific Plant Systems

## REACTOR COOLANT SYSTEMS

- **Requirement 49: Inventory of reactor coolant**
  - Provision shall be made for controlling the inventory, temperature and pressure of the reactor coolant to ensure that specified design limits are not exceeded in any operational state of the nuclear power plant, with due account taken of volumetric changes and leakage.
- **Requirement 50: Cleanup of reactor coolant**
  - Adequate facilities shall be provided at the nuclear power plant for the removal from the reactor coolant of radioactive substances, including activated corrosion products and fission products deriving from the fuel, and non-radioactive substances.

# Design of Specific Plant Systems

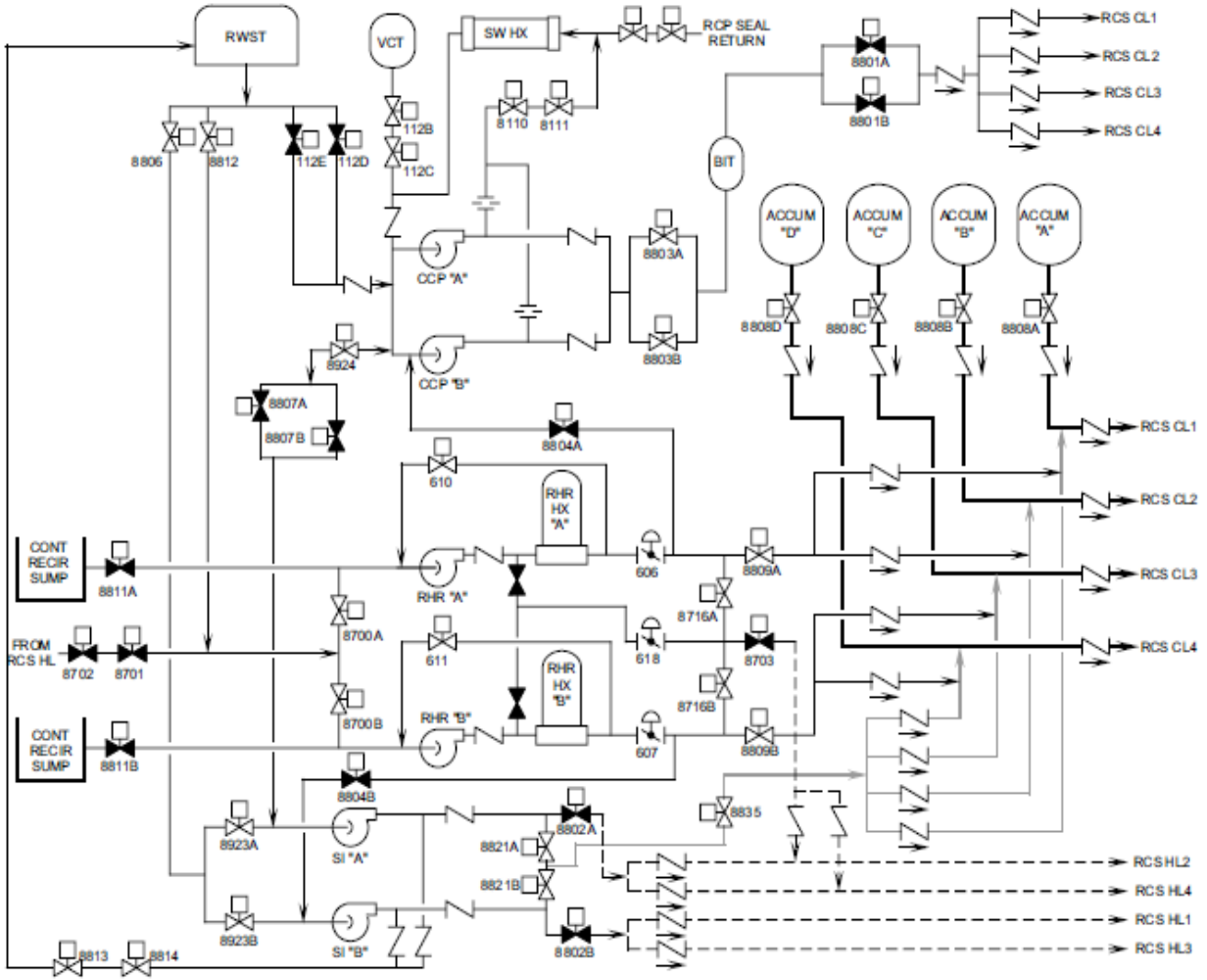
## REACTOR COOLANT SYSTEMS

- **Requirement 52: Emergency cooling of the reactor core**

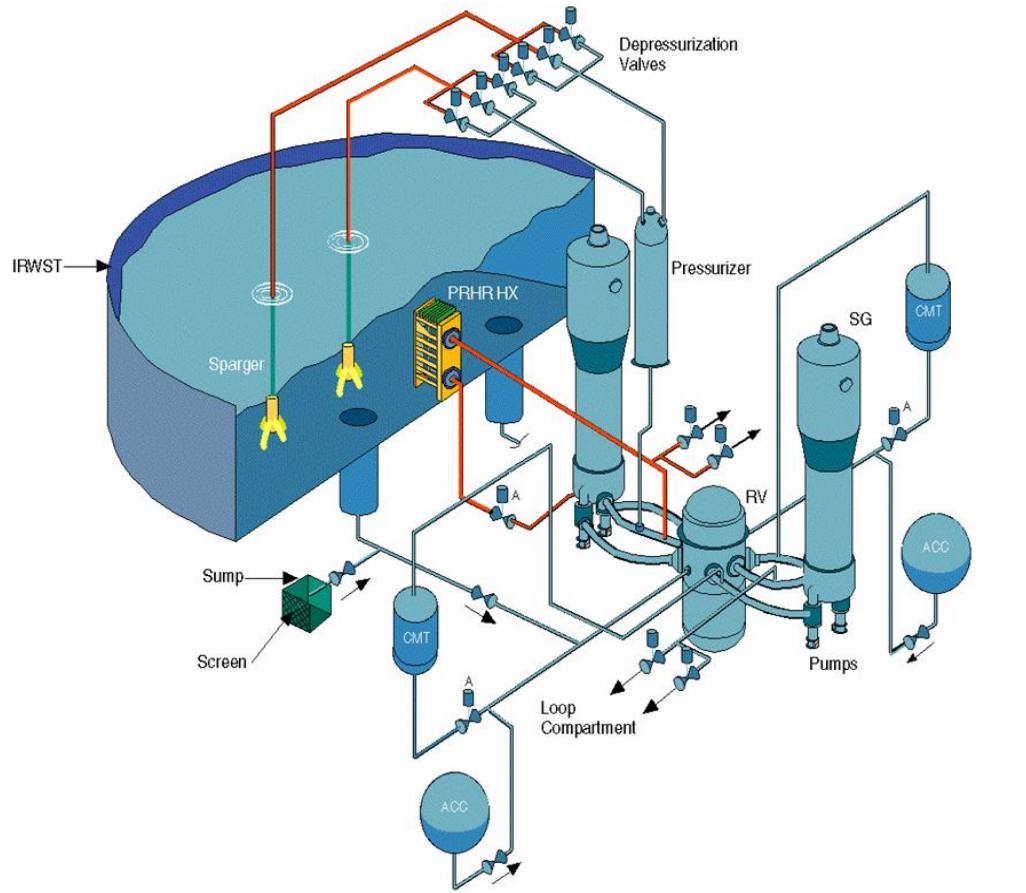
  Means of cooling the reactor core shall be provided to restore and maintain cooling of the fuel under accident conditions at the nuclear power plant even if the integrity of the pressure boundary of the primary coolant system is not maintained

  - The means for cooling of the reactor core shall ensure that:
    - The limiting parameters for the cladding or for integrity of the fuel will not be exceeded;
    - Possible chemical reactions are kept to an acceptable level;
    - The effectiveness of cooling of the reactor core compensates for possible changes in the fuel and in the internal geometry of the reactor core;
    - Cooling of the reactor core will be ensured for a sufficient time.

# ECCS in PWR


RWST
VCT
SW HX
RCP SEAL RETURN
8801A
8801B
RCS CL1
RCS CL2
RCS CL3
RCS CL4
8806
8812
112E
112D
112B
112C
8110
8111
BIT
ACCUM "D"
ACCUM "C"
ACCUM "B"
ACCUM "A"
8808D
8808C
8808B
8808A
CCP "A"
CCP "B"
8803A
8803B
8924
8807A
8807B
8804A
610
RHR HX "A"
RHR HX "B"
606
607
618
611
8809A
8809B
8716A
8716B
8703
CONT RECIR SUMP
8811A
8811B
FROM RCS HL
8702
8701
8700A
8700B
RHR "A"
RHR "B"
8804B
8835
8923A
8923B
SI "A"
SI "B"
8821A
8821B
8802A
8802B
RCS HL2
RCS HL4
RCS HL1
RCS HL3
8813
8814

# ECCS in AP1000



# Design of Specific Plant Systems

## REACTOR COOLANT SYSTEMS

- **Requirement 53: Heat transfer to an ultimate heat sink**

  The capability to transfer heat to an ultimate heat sink shall be ensured for all plant states.

  - Systems for transferring heat shall have adequate reliability for the plant states in which they have to fulfil the heat transfer function. This may require the use of a different ultimate heat sink or different access to the ultimate heat sink.

  - The heat transfer function shall be fulfilled for levels of natural hazards more severe than those to be considered for design taking into account the site hazard evaluation.

# Design of Specific Plant Systems

## CONTAINMENT STRUCTURE AND CONTAINMENT SYSTEM

- **Requirement 54: Containment system for the reactor**

  A containment system shall be provided to ensure or to contribute to the fulfilment of the following safety functions at the nuclear power plant: (1) confinement of radioactive substances in operational states and in accident conditions; (2) protection of the reactor against natural external events and human induced events; (3) radiation shielding in operational states and in accident conditions.

- **Requirement 55: Control of radioactive releases from the containment**

  The design of the containment shall be such as to ensure that any release of radioactive material from the nuclear power plant to the environment is as low as reasonably achievable, is below the authorized limits on discharges in operational states and is below acceptable limits in accident conditions.

# Design of Specific Plant Systems

## CONTAINMENT STRUCTURE AND CONTAINMENT SYSTEM

- **Requirement 56: Isolation of the containment**

  Each line that penetrates the containment at a nuclear power plant as part of the reactor coolant pressure boundary or that is connected directly to the containment atmosphere shall be automatically and reliably sealable in the event of an accident in which the leaktightness of the containment is essential to preventing radioactive releases to the environment that exceed acceptable limits.

- **Requirement 57: Access to the containment**

  Access by operating personnel to the containment at a nuclear power plant shall be through airlocks equipped with doors that are interlocked to ensure that at least one of the doors is closed during reactor power operation and in accident conditions.

# Design of Specific Plant Systems

## CONTAINMENT STRUCTURE AND CONTAINMENT SYSTEM

- **Requirement 58: Control of containment conditions**

  Provision shall be made to control the pressure and temperature in the containment at a nuclear power plant and to control any buildup of fission products or other gaseous, liquid or solid substances that might be released inside the containment and that could affect the operation of systems important to safety.

  - Sufficient flow routes between separate compartments inside the containment.
  - The capability to remove heat ensured by systems with sufficient reliability and redundancy. The design shall also include features to enable the safe use of non-permanent equipment for restoring the capability to remove heat.
  - the loss of the containment structural integrity shall be prevented in all plant states.
  - Design features to control fission products, hydrogen, oxygen and other substances that might be released into the containment shall be provided as necessary

# Design of Specific Plant Systems

## INSTRUMENTATION AND CONTROL SYSTEMS

- **Requirement 59: Provision of instrumentation**

  Instrumentation shall be provided for determining the values of all the main variables that can affect the fission process, the integrity of the reactor core, the reactor coolant systems and the containment at the nuclear power plant, for obtaining essential information on the plant that is necessary for its safe and reliable operation, for determining the status of the plant in accident conditions and for making decisions for the purposes of accident management.

- **Requirement 60: Control systems**

  Appropriate and reliable control systems shall be provided at the nuclear power plant to maintain and limit the relevant process variables within the specified operational ranges.

# Design of Specific Plant Systems

## INSTRUMENTATION AND CONTROL SYSTEMS

- **Requirement 61: Protection system**

  A protection system shall be provided at the nuclear power plant that has the capability to detect unsafe plant conditions and to initiate safety actions automatically to actuate the safety systems necessary for achieving and maintaining safe plant conditions.

- **Requirement 62: Reliability and testability of instrumentation and control systems**

  Instrumentation and control systems for items important to safety at the nuclear power plant shall be designed for high functional reliability and periodic testability commensurate with the safety function(s) to be performed.

# Design of Specific Plant Systems

## INSTRUMENTATION AND CONTROL SYSTEMS

- **Requirement 63: Use of computer based equipment in systems important to safety**

  If a system important to safety at the nuclear power plant is dependent upon computer based equipment, appropriate standards and practices for the development and testing of computer hardware and software shall be established and implemented throughout the service life of the system, and in particular throughout the software development cycle. The entire development shall be subject to a quality management system.

- **Requirement 64: Separation of protection systems and control systems**

  Interference between protection systems and control systems at the nuclear power plant shall be prevented by means of separation, by avoiding interconnections or by suitable functional independence.

# Design of Specific Plant Systems

## INSTRUMENTATION AND CONTROL SYSTEMS

- **Requirement 65: Control room**

  A control room shall be provided at the nuclear power plant from which the plant can be safely operated in all operational states, either automatically or manually, and from which measures can be taken to maintain the plant in a safe state or to bring it back into a safe state after anticipated operational occurrences and accident conditions.

  - Appropriate measures shall be taken for the protection of occupants of the control room, for a protracted period of time, against hazards such as high radiation levels resulting from accident conditions, release of radioactive material, fire, or explosive or toxic gases.
  - The design of the control room shall provide an adequate margin against levels of natural hazards more severe than those to be considered for design taking into account the site hazard evaluation.

# Design of Specific Plant Systems

## INSTRUMENTATION AND CONTROL SYSTEMS

- **Requirement 66: Supplementary control room**

  Instrumentation and control equipment shall be kept available, preferably at a single location (a supplementary control room) that is physically, electrically and functionally separate from the control room at the nuclear power plant. The supplementary control room shall be so equipped that the reactor can be placed and maintained in a shutdown state, residual heat can be removed, and essential plant variables can be monitored if there is a loss of ability to perform these essential safety functions in the control room.

- **Requirement 67: Emergency response facilities on the site**

  The nuclear power plant shall include the necessary emergency response facilities on the site. Their design shall be such that personnel will be able to perform expected tasks for managing an emergency under conditions generated by accidents and hazards

# Design of Specific Plant Systems

## EMERGENCY POWER SUPPLY

- **Requirement 68: Design for withstanding the loss of off-site power**

  The design of a nuclear power plant shall include an emergency power supply capable of supplying the necessary power in anticipated operational occurrences and design basis accidents, in the event of the loss of off-site power. The design shall include an alternate power source to supply the necessary power in design extension conditions

  - The design specifications for the emergency power supply and for the alternate power source at the nuclear power plant shall include the requirements for capability, availability, duration of the required power supply, capacity and continuity.
  - The alternate power source shall be capable of supplying the necessary power to preserve the integrity of the reactor coolant system and to prevent significant damage to the core and to spent fuel in the event of the loss of off-site power combined with failure of the emergency power supply.
  - **Equipment that is necessary to mitigate the consequences of melting of the reactor core shall be capable of being supplied by any of the available power sources**.

# Design of Specific Plant Systems

## SUPPORT AND AUXILIARY SYSTEMS

- **Requirement 69: Performance of supporting systems and auxiliary systems**

  The design of supporting systems and auxiliary systems shall be such as to ensure that the performance of these systems is consistent with the safety significance of the system or component that they serve at the nuclear power plant.

- **Requirement 70: Heat transport systems**

  Auxiliary systems shall be provided as appropriate to remove heat from systems and components at the nuclear power plant that are required to function in operational states and in accident conditions.

# Design of Specific Plant Systems

## SUPPORT AND AUXILIARY SYSTEMS

- **Requirement 71: Process sampling systems and post-accident sampling systems**

  Process sampling systems and post-accident sampling systems shall be provided for determining, in a timely manner, the concentration of specified radionuclides in fluid process systems, and in gas and liquid samples taken from systems or from the environment, in all operational states and in accident conditions at the nuclear power plant.

- **Requirement 72: Compressed air systems**

  The design basis for any compressed air system that serves an item important to safety at the nuclear power plant shall specify the quality, flow rate and cleanness of the air to be provided.

# Design of Specific Plant Systems

## SUPPORT AND AUXILIARY SYSTEMS

- **Requirement 73: Air conditioning systems and ventilation systems**

  Systems for air conditioning, air heating, air cooling and ventilation shall be provided as appropriate in auxiliary rooms or other areas at the nuclear power plant to maintain the required environmental conditions for systems and components important to safety in all plant states.

- **Requirement 74: Fire protection systems**

  Fire protection systems, including fire detection systems and fire extinguishing systems, fire containment barriers and smoke control systems, shall be provided throughout the nuclear power plant, with due account taken of the results of the fire hazard analysis.

# Design of Specific Plant Systems

## SUPPORT AND AUXILIARY SYSTEMS

- **Requirement 75: Lighting systems**

  Adequate lighting shall be provided in all operational areas of the nuclear power plant in operational states and in accident conditions.

- **Requirement 76: Overhead lifting equipment**

  Overhead lifting equipment shall be provided for lifting and lowering items important to safety at the nuclear power plant, and for lifting and lowering other items in the proximity of items important to safety.

# Design of Specific Plant Systems

## OTHER POWER CONVERSION SYSTEMS

- **Requirement 77: Steam supply system, feedwater system and turbine generators**

  The design of the steam supply system, feedwater system and turbine generators for the nuclear power plant shall be such as to ensure that the appropriate design limits of the reactor coolant pressure boundary are not exceeded in operational states or in accident conditions.

  - The design of the steam supply system shall provide for appropriately rated and qualified steam isolation valves capable of closing under the specified conditions in operational states and in accident conditions.
  - The steam supply system and the feedwater systems shall be of sufficient capacity and shall be designed to prevent anticipated operational occurrences from escalating to accident conditions

# Design of Specific Plant Systems

## TREATMENT OF RADIOACTIVE EFFLUENTS AND RADIOACTIVE WASTE

- **Requirement 78: Systems for treatment and control of waste**

  Systems shall be provided for treating solid radioactive waste and liquid radioactive waste at the nuclear power plant to keep the amounts and concentrations of radioactive releases below the authorized limits on discharges and as low as reasonably achievable.

- **Requirement 79: Systems for treatment and control of effluents**

  Systems shall be provided at the nuclear power plant for treating liquid and gaseous radioactive effluents to keep their amounts below the authorized limits on discharges and as low as reasonably achievable.

# Design of Specific Plant Systems

## FUEL HANDLING AND STORAGE SYSTEMS

- **Requirement 80: Fuel handling and storage systems**

  Fuel handling and storage systems shall be provided at the nuclear power plant to ensure that the integrity and properties of the fuel are maintained at all times during fuel handling and storage.

# Design of Specific Plant Systems

## RADIATION PROTECTION

- **Requirement 81: Design for radiation protection**

  Provision shall be made for ensuring that doses to operating personnel at the nuclear power plant will be maintained below the dose limits and will be kept as low as reasonably achievable, and that the relevant dose constraints will be taken into consideration.

- **Requirement 82: Means of radiation monitoring**

  Equipment shall be provided at the nuclear power plant to ensure that there is adequate radiation monitoring in operational states and design basis accident conditions and, as far as is practicable, in design extension conditions.

# Thank You !