Engineering Factors for NPPs

Manwoong KIM
m.kim@kins.re.kr

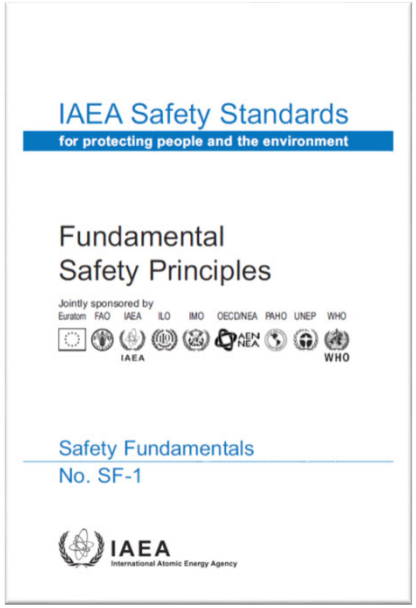
CONTENTS

I. Need for Safety Assessment

SF1 Fundamental Safety Principles

- The fundamental safety objective is to protect people and the environment from harmful effects of ionizing radiation.
- To ensure that facilities are operated and activities conducted so as to achieve the highest standards of safety that can reasonably be achieved, measures have to be taken:
  - To restrict the likelihood of events that might lead to a loss of control over a nuclear reactor core, nuclear chain reaction, radioactive source or any other source of radiation;
  - To mitigate the consequences of such events if they were to occur;
  - To control the radiation exposure of people and the release of radioactive material to the environment.

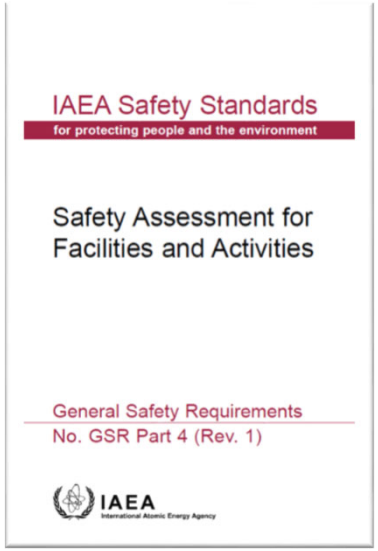
Ref. : IAEA Safety Standard Series No. SF-1



GSR Part 4 Safety Assessment for Facilities and Activities

Requirement 4: Purpose of the safety assessment

The primary purposes of the safety assessment shall be to determine whether an adequate level of safety has been achieved for a facility or activity and whether the basic safety objectives and safety criteria established by the designer, the operating organization and the regulatory body, in compliance with the requirements for protection and safety as established in Radiation Protection and Safety of Radiation Sources: International Basic Safety Standards, IAEA Safety Standards Series No. GSR Part 3, have been fulfilled.

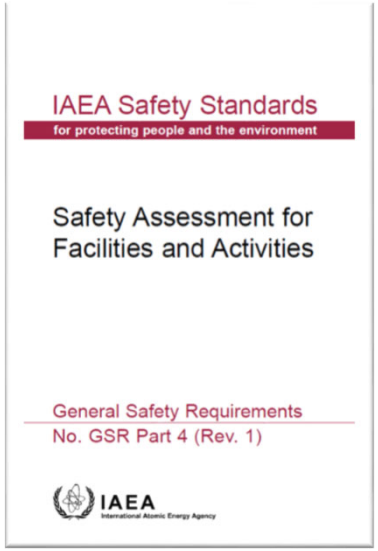


GSR Part 4 Safety Assessment for Facilities and Activities

Requirement 3: Responsibility for the safety assessment

The responsibility for carrying out the safety assessment shall rest with the responsible legal person; that is, the person or organization responsible for the facility or activity.

- Generally, the person or organization authorized (licensed) to operate the facility.
- The operating organization shall be responsible for the safety assessment.



Safety Assessment for Facilities

Safety Assessment

Safety Analysis

Two complementary methods

Deterministic Safety Analysis (DSA)

Predicts the response to postulated events with predetermined assumptions; checks fulfilment of acceptance criteria

Probabilistic Safety Analysis (PSA)

Combines the likelihood of initiating events, potential scenarios and their consequences into estimation of CDF, source term or overall risk

Safety Approach

- **Defence in depth**
- **Safety Margin**
- **Multiple barriers**

Safety Features

- **Site characteristics**
- **Engineering aspects**
- **Safety function**
- **Human factors**
- **Long-term safety**
- **Radiation protection**

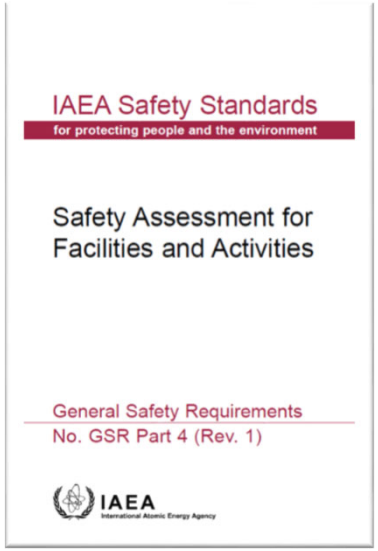
- **Proven engineering practices**
- **Redundancy, diversity**
- **Single failure criterion**
- **Safety classification**
- **Equipment qualification**
- **Selection of materials**

GSR Part 4 Safety Assessment for Facilities and Activities

Requirement 10: Assessment of engineering aspects

It shall be determined in the safety assessment whether a facility or activity uses, to the extent practicable, structures, systems and components of robust and proven design.

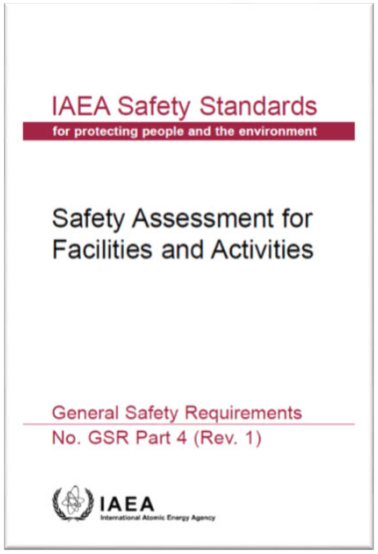
- 4.27 Relevant operating experience, including results of root cause analysis of operational occurrences, accident conditions and accident precursors where appropriate, shall be taken into account.
- 4.28. The design principles applied will depend on the type of facility but could give rise to requirements to incorporate defence in depth, (1) multiple barriers to the release of radioactive material, and (2) safety margins, and (3) to provide redundancy, diversity and equipment qualification in the design of safety systems."



GSR Part 4 Safety Assessment (cont'd)

4.30. It shall be determined in the safety assessment whether a suitable safety classification scheme has been formulated and applied to structures, systems and components.

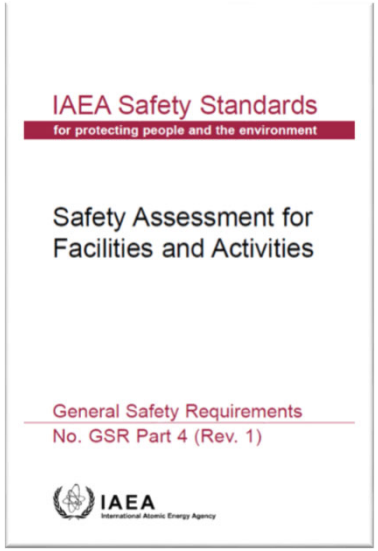
4.32. The internal events that could arise for a facility shall be addressed in the safety assessment, and it shall be demonstrated whether the structures, systems and components are able to perform their safety functions under the loads induced by normal operation and the anticipated operational occurrences and accident conditions



GSR Part 4 Safety Assessment (cont'd)

4.33. It shall be determined in the safety assessment whether the materials used are suitable for their purpose with regard to the standards specified in the design, and for the conditions that arise during normal operation and following anticipated operational occurrences or accident conditions

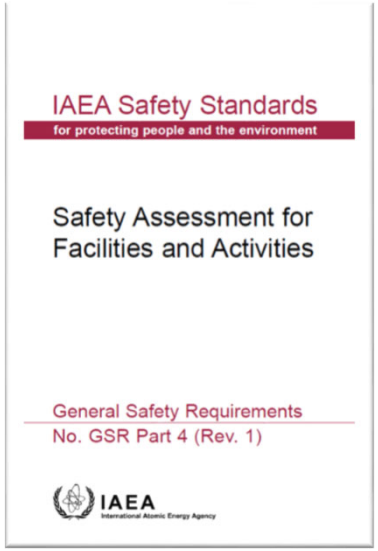
4.34. It shall be addressed in the safety assessment whether preference has been given to a fail-safe design or, if this is not practicable, whether an effective means of detecting failures that occur has been incorporated wherever appropriate.



GSR Part 4 Safety Assessment (cont'd)

4.33. It shall be determined in the safety assessment whether the materials used are suitable for their purpose with regard to the standards specified in the design, and for the conditions that arise during normal operation and following anticipated operational occurrences or accident conditions

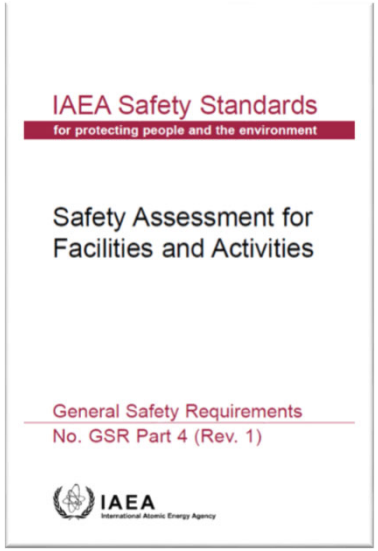
4.35. It shall be determined in the safety assessment whether any time related aspects, such as ageing and wear, or life limiting factors, such as cumulative fatigue, embrittlement, corrosion, chemical decomposition and radiation induced damage, have been adequately addressed.



GSR Part 4 Safety Assessment (cont'd)

4.36. It shall be determined in the safety assessment whether equipment essential to safety has been qualified to a sufficiently high level that it will be able to perform its safety function in the conditions that would be encountered in normal operation, and following anticipated operational occurrences and accident conditions

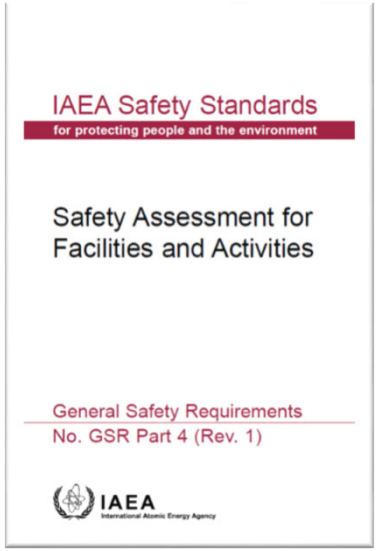
4.36A. For sites with multiple facilities or multiple activities, account shall be taken in the safety assessment of the effects of external events on all facilities and activities.



GSR Part 4 Safety Assessment (cont'd)

4.36B. For facilities on a site that would share resources (whether human resources or material resources) in accident conditions,

4.37. The provisions made for the decommissioning and dismantling of a facility or for the closure of a disposal facility for radioactive waste shall be specified,



GSG-13 Functions and Processes of the Regulatory Body for Safety: recommendations

Verification of the safety analysis

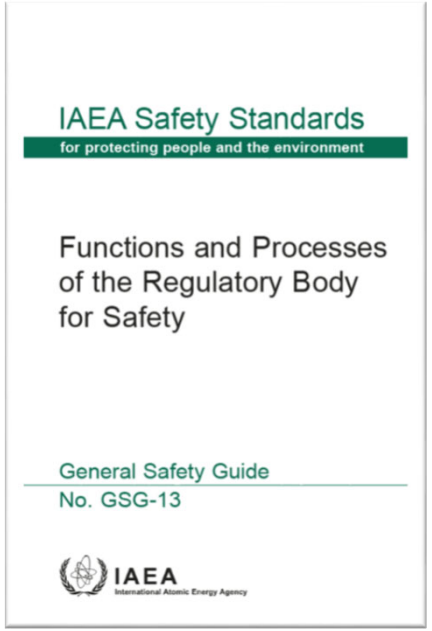
3.195 The review and assessment process by the regulatory body consists of examination of the submissions from the authorized party on its management arrangements and operational procedures and verification of the safety analysis……. In carrying out the review and assessment, the regulatory body may find it useful to perform its own analyses or research. The following subsections deal with major aspects of such verification.

3.196 In the verification of the safety analysis for the facility or activity, the regulatory body should determine whether the authorized party has defined criteria that meet the safety objectives and requirements relating to:

(a) Engineering design;

(b) Operational and managerial aspects;

(c) Normal operation, anticipated operational occurrences and accident conditions.



II. Safety Approach

Safety Assessment for Facilities

Safety Assessment

Safety Analysis

Two complementary methods

Deterministic Safety Analysis (DSA)

Predicts the response to postulated events with predetermined assumptions; checks fulfilment of acceptance criteria

Probabilistic Safety Analysis (PSA)

Combines the likelihood of initiating events, potential scenarios and their consequences into estimation of CDF, source term or overall risk

Safety Approach

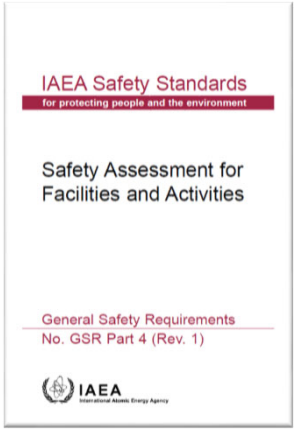
- **Defence in depth**
- **Safety Margin**
- **Multiple barriers**

Safety Features

- **Site characteristics**
- **Engineering aspects**
- **Safety function**
- **Human factors**
- **Long-term safety**
- **Radiation protection**

- **Proven engineering practices**
- **Redundancy, diversity**
- **Single failure criterion**
- **Safety classification**
- **Equipment qualification**
- **Selection of materials**

2. Safety Approach: (1) Defence in depth



GSR Part 4 Safety Assessment

Requirement 13: Assessment of defence in depth

It shall be determined in the assessment of defence in depth whether adequate provisions have been made at each of the levels of defence in depth.

4.45. It shall be determined in the assessment of defence in depth whether adequate provisions have been made at each of the levels of defence in depth to ensure that the person or organization responsible for the facility can:

(a) Address deviations from normal operation or, in the case of a disposal facility, from its expected evolution in the long term;

(b) Detect and terminate safety related deviations from normal operation or from its expected evolution in the long term, should deviations occur;

(c) Control accidents within the limits specified in the design;

(d) Specify measures to mitigate the consequences of accidents that exceed design limits;

(e) Mitigate radiation risks associated with possible releases of radioactive material.

(1) Defence in depth (cont'd)

4.46. The necessary layers of protection, including physical barriers to confine radioactive material at specific locations, and the necessary supporting administrative controls for achieving defence in depth shall be identified in the safety assessment. This shall include identification of:

(a) Safety functions that must be fulfilled;

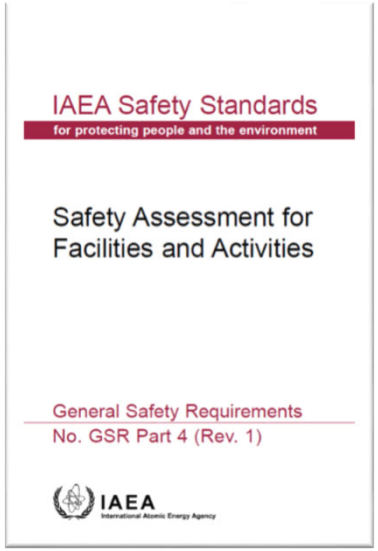
(b) Potential challenges to these safety functions;

(c) Mechanisms that give rise to these challenges, and the necessary responses to them;

(d) Provisions made to prevent these mechanisms from occurring;

(e) Provisions made to identify or monitor deterioration caused by these mechanisms, if practicable;

(f) Provisions for mitigating the consequences if the safety functions fail.



Multiple Physical Barriers and DID Levels

- IAEA INSAG-12

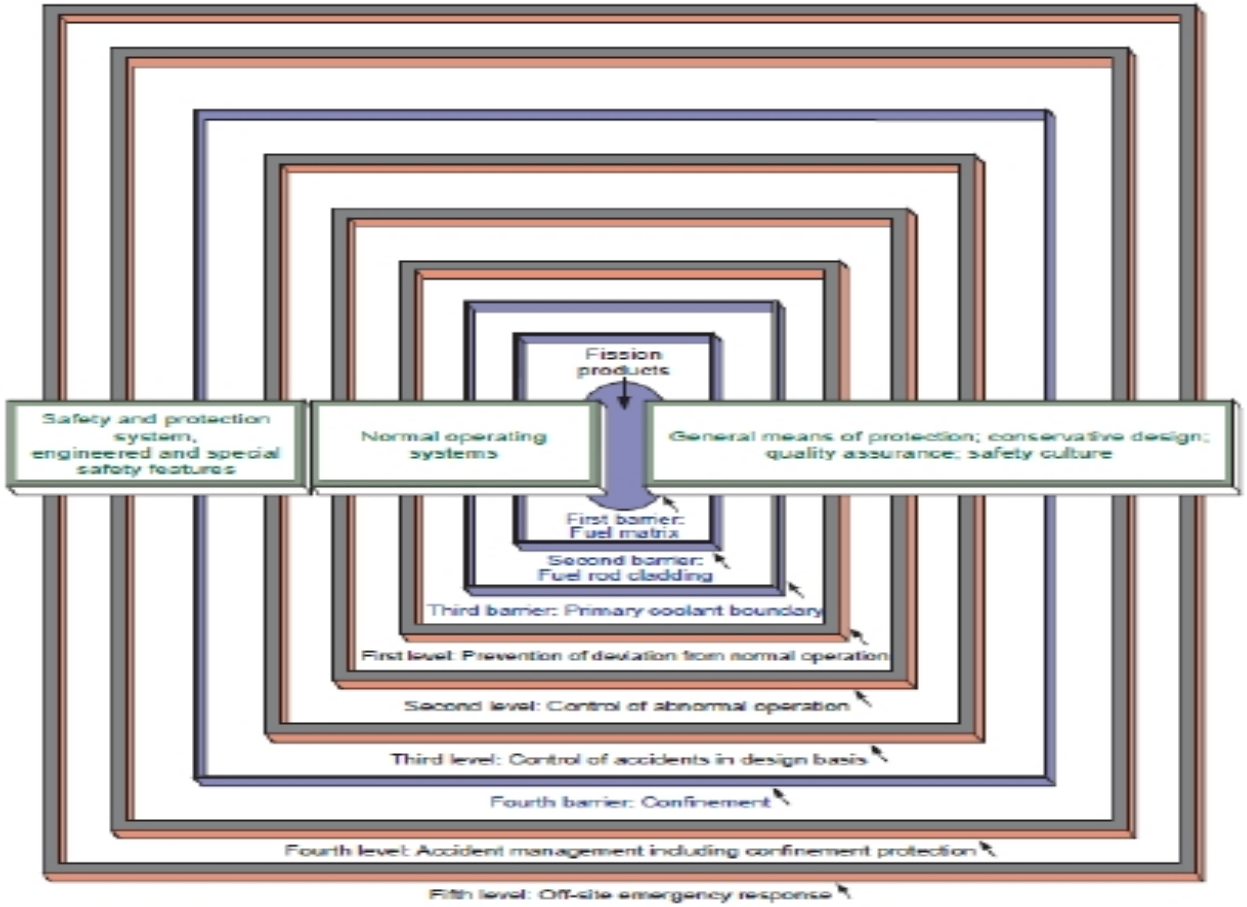


FIG. 4. The relation between physical barriers and levels of protection in defence in depth.

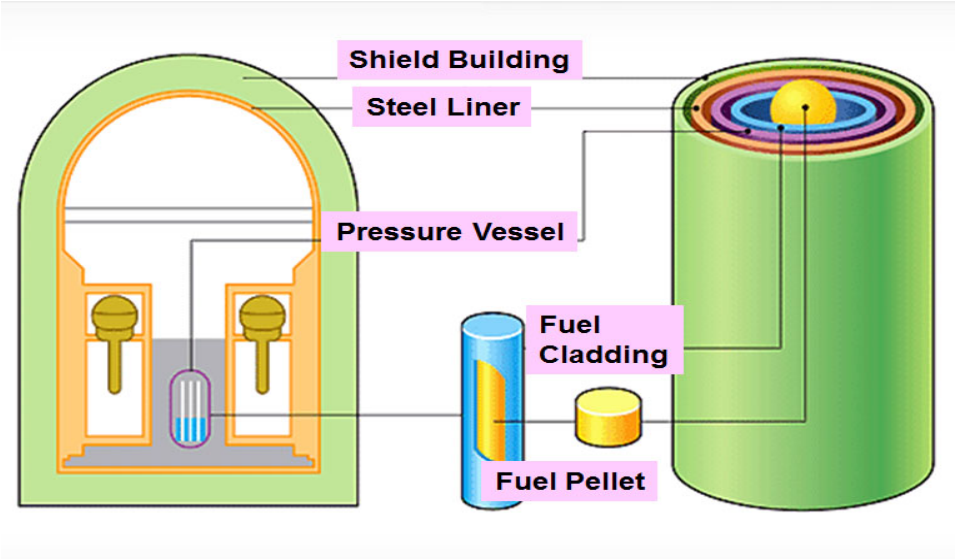
Multiple Physical Barriers of a NPP

- Multiple physical barriers to prevent radioactive material release
  - Fuel pellet
  - Fuel cladding
  - Reactor vessel and coolant pipe
  - Containment Building

RB base slab 10.06m thickness(max.),
ID 45.72m, height 76.66m, wall thickness 1.22m,
dome thickness 1.07m (in case of Shin-KORI 3/4)

Fuel cladding(ZIRLO)
thickness 0.053cm

Component	MNB 3641 [NB-3641]	
	Min. Required Thk. (in)	Min. Design Thk. (in)
42″ Pipe	3.34	3.875



Levels of Defence in Depth (INSAG-10)

Level	Objective	Essential Means
Level 1	• Prevention of abnormal operation and failures.	• Conservative design • High quality in construction operation and operation
Level 2	• Control of abnormal operation and detection of failures.	• Control, limiting and protection systems and other surveillance features
Level 3	• Control of accidents within the design basis.	• Engineered Safety Features and accident procedure
Level 4	• Control of severe plant conditions, including prevention of accident progression and mitigation of the consequences of severe accidents.	• Complementary measures and accident Management
Level 5	• Mitigation of radiological consequences of significant releases of radioactive material	• Off-site Emergency response

Defence in Depth applied to NPPs: INSAG-12

Strategy	Accident prevention			Accident mitigation	
Operational state of the plant	Normal operation	Anticipated operational occurrences	Design basis and complex operating states	Severe accidents beyond the design basis	Post-severe accident situation
Level of defence in depth	Level 1	Level 2	Level 3	Level 4	Level 5
Objective	Prevention of abnormal operation and failure	Control of abnormal operation and detection of failures	Control of accidents below the severity level postulated in the design basis	Control of severe plant conditions, including prevention of accident progression, and mitigation of the consequences of severe accidents, including confinement protection	Mitigation of radiological consequences of significant releases of radioactive materials
Essential features	Conservative design and quality in construction and operation	Control, limiting and protection systems and other surveillance features	Engineered safety features and accident procedures	Complementary measures and accident management, including confinement prodection	Off-site emergency response
Control	Normal operating activities		Control of accidents in design basis	Accident management	
Procedures	Normal operating procedures		Emergency operating procedures	Ultimate part of emergency operating procedures	
Response	Normal operating systems		Engineered safety features	Special design features	Off-site emergency preparations
Condition of barriers	Area of specified acceptable fuel design limit		Fuel failure; Severe fuel damage	Fuel melt; Uncontrolled fuel melt	Loss of confinement
Colour code	NORMAL		POSTULATED ACCIDENTS		EMERGENCY

(2) Safety Margin

GSR Part 4 Safety Assessment

DEFENCE IN DEPTH AND SAFETY MARGINS

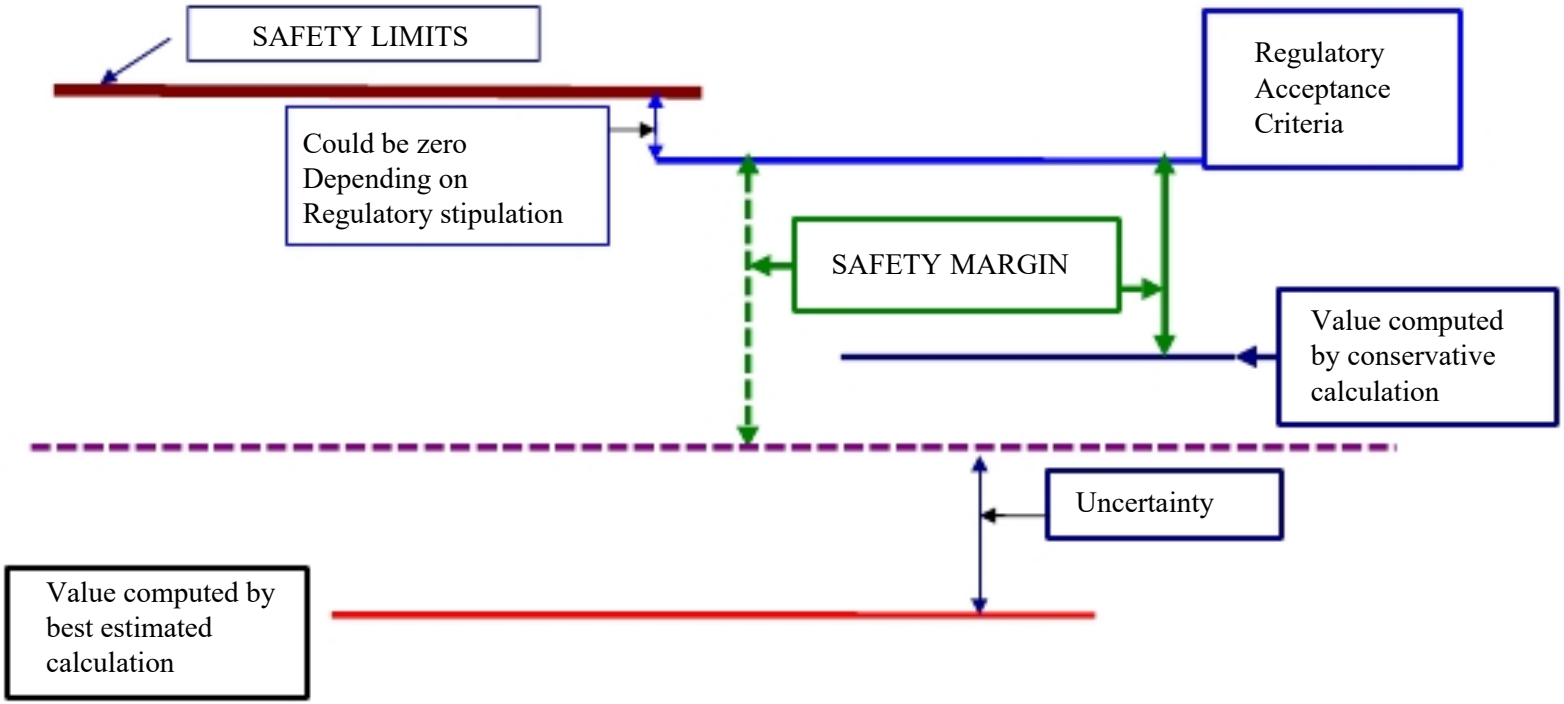
4.48. It shall be determined in the safety assessment whether there are adequate safety margins in the design and operation of the facility, or in the conduct of the activity, in normal operation and in anticipated operational occurrences or accident conditions such that there is a wide margin to failure of any structures, systems and components for any of the anticipated operational occurrences or any possible accident conditions. Safety margins are typically specified in codes and standards as well as by the regulatory body.

4.48A. Where practicable, the safety assessment shall confirm that there are adequate margins to avoid cliff edge effects[9] that would have unacceptable consequences.

9 'cliff edge effect' is an instance of severely abnormal conditions caused by an abrupt transition from one status of a facility to another following a small deviation in a parameter or a small variation in an input value.

(2) Safety Margins - Definition

- The safety margin is defined as the difference or ratio in physical units between the limiting value of an assigned parameter the surpassing of which leads to the failure of a system or component, and the actual value of that parameter in the plant.



III. Engineering Aspects

Safety Assessment for Facilities

Safety Assessment

Safety Analysis

Two complementary methods

Deterministic Safety Analysis (DSA)

Predicts the response to postulated events with predetermined assumptions; checks fulfilment of acceptance criteria

Probabilistic Safety Analysis (PSA)

Combines the likelihood of initiating events, potential scenarios and their consequences into estimation of CDF, source term or overall risk

Safety Approach

- **Multiple barriers**
- **Defence in depth**
- **Safety Margin**

Safety Features

- **Site characteristics**
- **Engineering aspects**
- **Safety function**
- **Human factors**
- **Long-term safety**
- **Radiation protection**

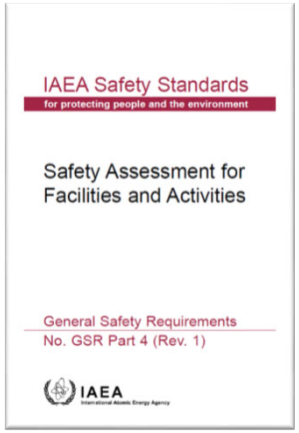
- **Proven engineering practices**
- **Engineering design rules**
- **Safety function(Redundancy, diversity)**
- **Single failure criterion**
- **Safety classification**
- **Equipment qualification**
- **Selection of materials**

(1) Proven engineering practices

GSR Part 4 Safety Assessment

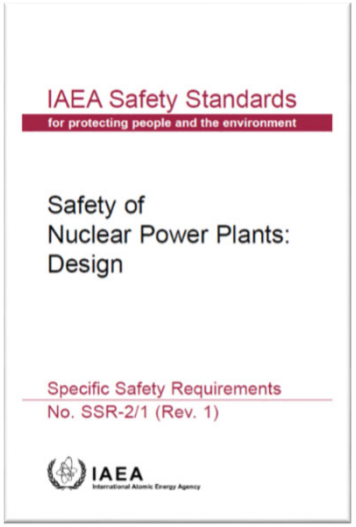
Requirement 10: Assessment of engineering aspects

4.29 Where innovative improvements beyond current practices have been incorporated into the design, it has to be determined in the safety assessment whether compliance with the safety requirements has been demonstrated by an appropriate programme of research, analysis and testing complemented by a subsequent programme of monitoring during operation.



(2) Engineering design rules

- SSR-2/1 Requirement 18: Engineering design rules
  - "The engineering design rules for items important to safety at a nuclear power plant shall be specified and shall comply with the relevant national or international codes and standards and with proven engineering practices, with due account taken of their relevance to nuclear power technology."


IAEA Safety Standards
for protecting people and the environment

Safety of
Nuclear Power Plants:
Design

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

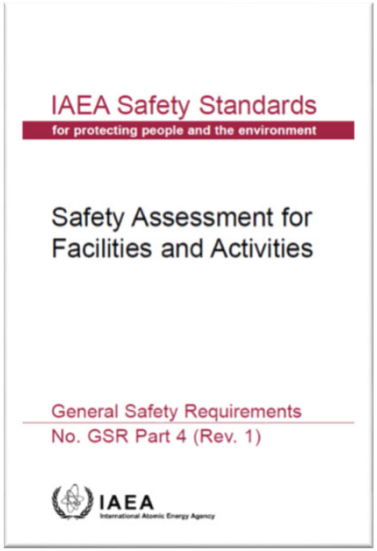
IAEA

7. Engineering design rules (cont'd)

- SSR-2/1 Requirement 18: Engineering design rules
  - Methods to ensure a robust design shall be applied, and proven engineering practices shall be adhered to in the design of a nuclear power plant to ensure that the fundamental safety functions are achieved for all operational states and for all accident conditions.

(3) Safety Function

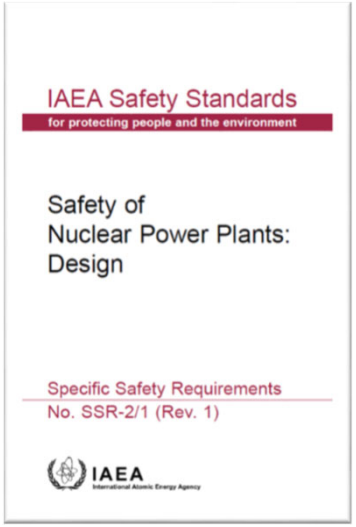
Safety functions are functions that are necessary to be performed for the facility or activity to prevent or to mitigate radiological consequences of normal operation, anticipated operational occurrences and accident conditions. These functions can include control of reactivity, removal of heat from radioactive material, confinement of radioactive material and shielding, depending on the nature of the facility or activity.



(3) Safety Function (cont'd)

SSR-2/1 (Safety of NPP: Design) lists 82 Requirements to be fulfilled by the design of a NPP:

- The capability to **safely shut down(Req. 46)** the reactor and maintain it in a safe shutdown condition during and after appropriate operational states and accident conditions;
- The capability to **remove residual heat(Req. 51)** from the reactor core after shutdown, and during and after appropriate operational states and accident conditions;
- The capability to reduce the potential for the **release of radioactive material (Req. 34,48)**and to ensure that any releases are within prescribed limits during and after operational states and within acceptable limits during and after design basis accidents.

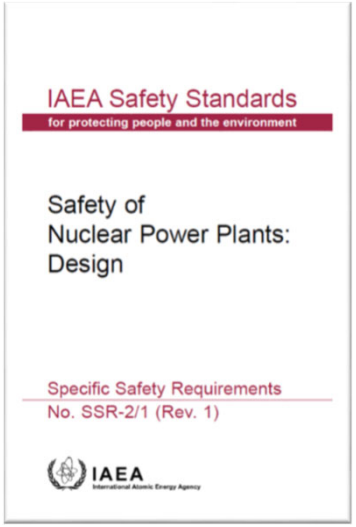


(3) Safety Function (cont'd)

Requirement 7: Assessment of safety functions

All safety functions associated with a facility or activity shall be specified and assessed.

4.21 It shall be determined in the assessment whether the structures, systems and components and the barriers that are provided to perform the safety functions have an adequate level of reliability, redundancy, diversity, separation, segregation, independence and equipment qualification, as appropriate, and whether potential vulnerabilities have been identified and eliminated.



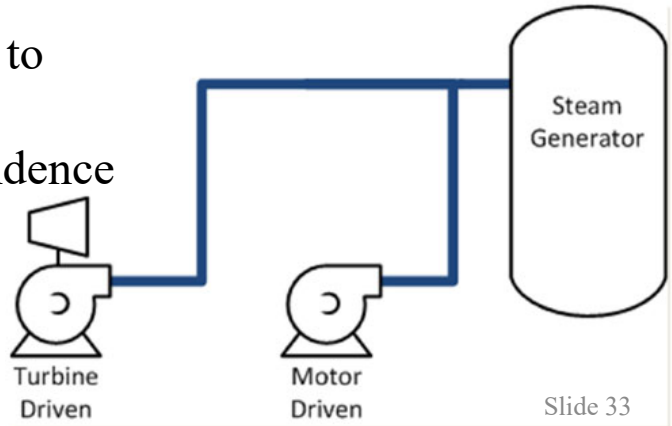
(3-1) Diversity

- Diversity is applied to redundant systems or components that perform the same safety function by incorporating different attributes into the systems or components.
- Such attributes could be different principles of operation, different physical variables, different conditions of operation, or production by different manufacturers.

SSR 2/1 Design

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



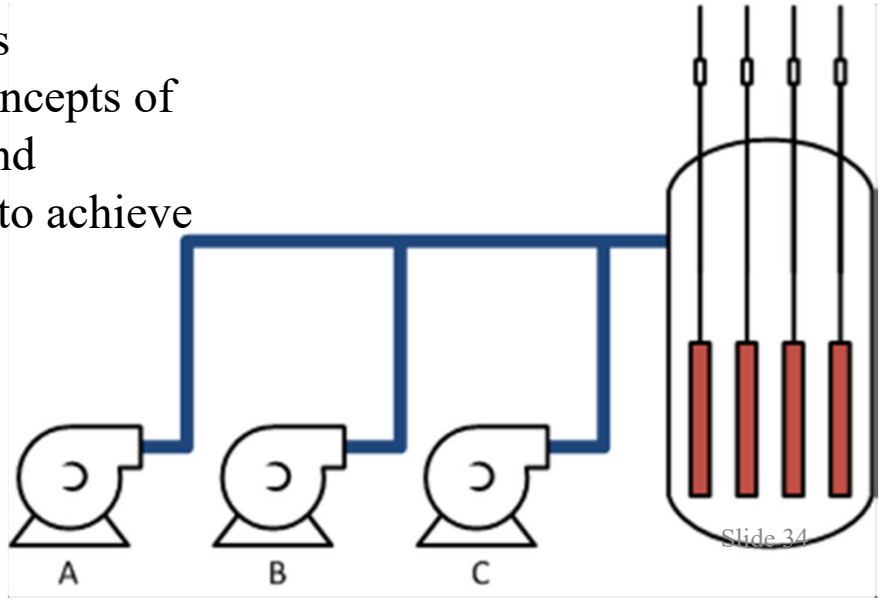
(3-2) Redundancy

- Redundancy is the use of more than the minimum number of sets of equipment to fulfil a given safety function. Redundancy enables failure or unavailability of at least one set of equipment to be tolerated without loss of the function

SSR 2/1 Design

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.



(3-3) Physical separation and independence

- Physical separation and independence of safety systems
  - Independence is accomplished in the design of systems by using functional isolation and physical separation
  - Functional isolation to reduce the likelihood of adverse interaction between equipment and components of redundant or connected systems resulting from normal or abnormal operation or failure of any component in the systems.
  - Physical separation in the system layout and design to increase assurance that independence will be achieved in relation to certain common cause failures.

(3-3) Physical separation and independence (cont'd)

SSR-2/1 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."

5.33 Safety system equipment (including cables and raceways) shall be readily identifiable in the plant for each redundant element of a safety system.

(4) Single failure criterion

Single failure

A failure that results in the loss of capability of a system or component to perform its intended safety function(s) and any consequential failure(s) that result from it. The single failure criterion is a criterion (or requirement) applied to a system such that it must be capable of performing its task in the presence of any single failure.

(4) Single Failure Criterion (cont'd)

SSR-2/1 Requirement 25: Single failure criterion

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

5.39. Spurious action shall be considered to be one mode of failure when applying the single failure criterion to a safety group or safety system.

5.40. The design shall take due account of the failure of a passive component, unless it has been justified in the single failure analysis with a high level of

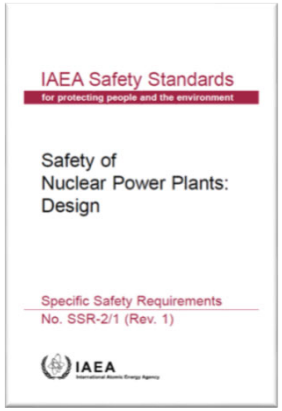
confidence that a failure of that component is very unlikely and that its function would remain unaffected by the postulated initiating event.

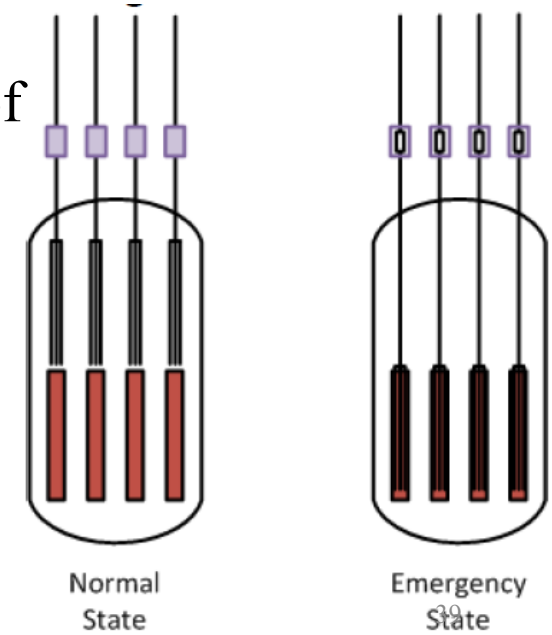
(5) Fail-safe design

SSR-2/1 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.

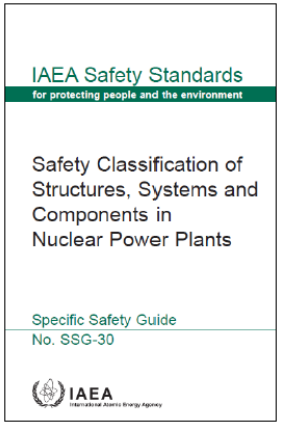
5.41 Systems and components important to safety shall be designed for fail-safe behaviour, as appropriate, so that their failure or the failure of a support feature does not prevent the performance of the intended safety function.





(6) Safety classification

- SSR-2/1 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 significance with regard to safety is mainly established considering:
    - the safety function(s) to be performed by the item
    - the consequences of failure to perform its function
    - the probability to be called upon to perform its function
    - The safety classification affects the design rules, the quality requirements, the manufacturing process, the maintenance requirements and the cost!



(7) Qualification of items important to safety

- SSR-2/1 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."

III. Summary

III. Summary (Recapping)

1. Safety Approach
   - Defence in depth (Multiple Barriers)
   - Safety margin
2. Engineering aspects
   - Proven engineering practices
   - Engineering Design Rules
   - Safety function
     - Redundancy
     - Diversity
     - Fail-safe design
     - Physical separation and independence of safety systems
   - Single Failure Criteria
   - Safety classification
   - Equipment qualification

III. Summary (cont'd)

- The assessment of engineering factors is a cornerstone of the verification of safety by taking into account the established criteria and proven engineering practices.
- This assessment along with the deterministic and probabilistic approaches forms the basis to verify compliance with the safety objectives and criteria.

References

1. International Atomic Energy Agency, Defence in Depth in Nuclear Safety, INSAG-10, 1996
2. International Atomic Energy Agency, Basic Safety Principles for Nuclear Power Plants 75-INSAG-3 Rev.1 INSAG-12, 1999.
3. OECD Nuclear Energy Agency, Implementation of Defence in Depth at Nuclear Power Plants, Lessons Learnt from the Fukushima Daiichi Accident, 2016
4. Western European Nuclear Regulators Associations, Safety of a New NPP designs, WENRARHWG Report, March 2013
5. International Atomic Energy Agency, Safety Margins of Operating Reactors, IAEA-TECDOC-1332, January 2003.