Joint KINS-IAEA-ANNuR/ANSN/FNRBA
BPTC Course on Nuclear Safety,
19 ~ 30 September 2022, KINS, Korea

Engineering Factors for NPPs

Manwoong KIM
m.kim@kins.re.kr

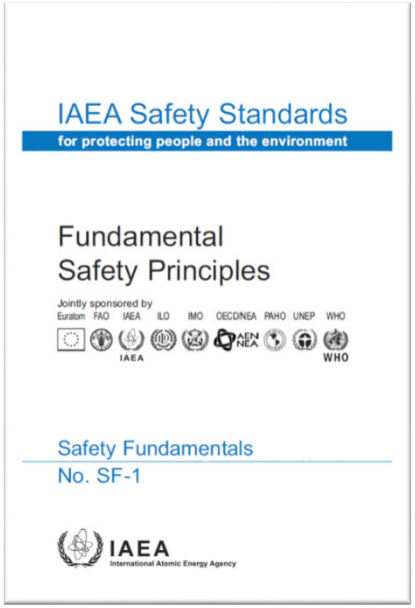
Presentation Outline

1. Needs for Safety Assessment
   - Safety Analysis (covered by another lectures)
   - Safety Approach
2. Safety Approach
   - Multiple barriers
   - Defence in depth
   - Safety Margin
3. Engineering Aspects
4. Summary

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.

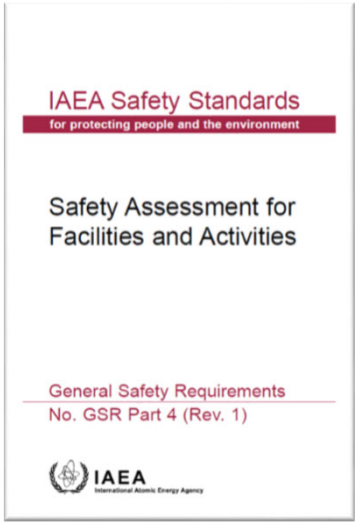


GSR Part 4 Safety Assessment for Facilities and Activities

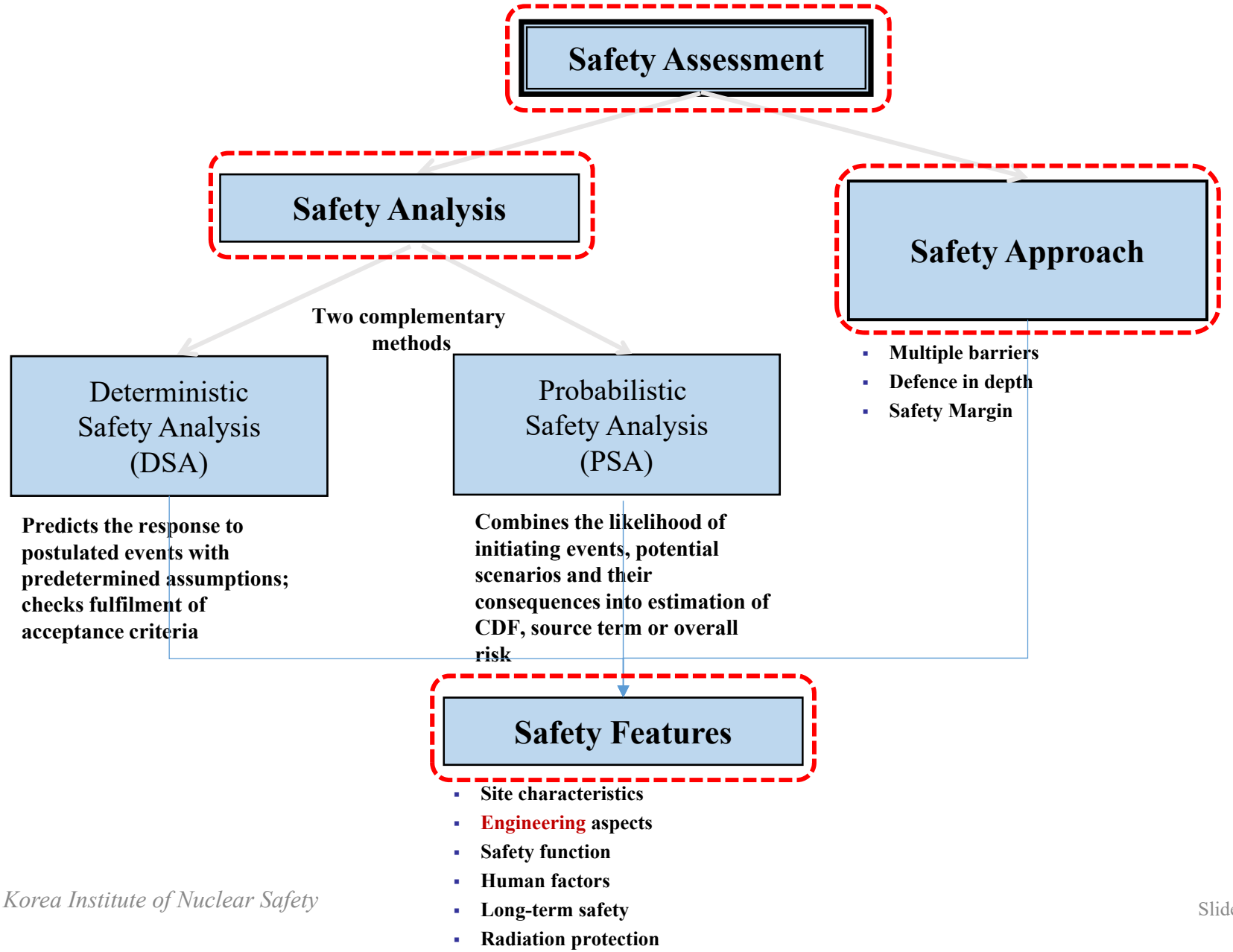
Requirement 3: Responsibility for the safety assessment

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

- Generally, the operating organization shall be responsible for the safety assessment.



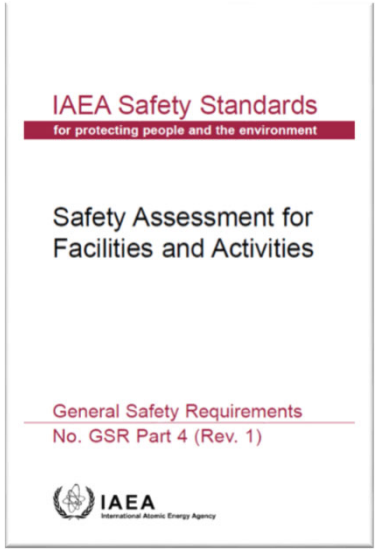
Safety Assessment for Facilities



GSR Part 4 Safety Assessment for Facilities and Activities

Requirement 10: Assessment of engineering aspects

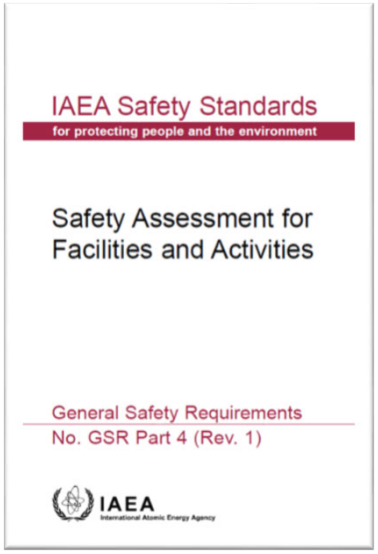
It shall be determined in the safety assessment whether a facility or activity uses, to the extent practicable, structures, systems and components of robust and proven design.



- The design principles applied will depend on the type of facility but could give rise to requirements to incorporate;
  - defence in depth, multiple barriers to the release of radioactive material,
  - safety margins, and
  - to provide redundancy, diversity and equipment qualification in the design of safety systems.

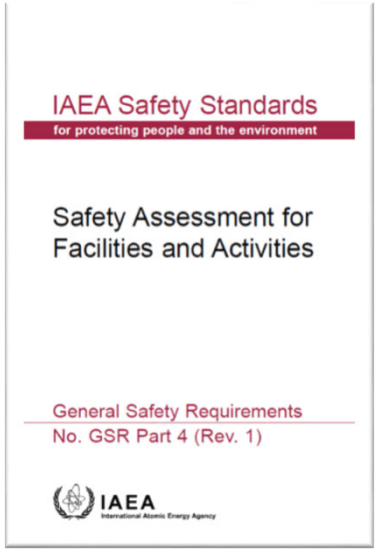
GSR Part 4 Safety Assessment (cont'd)

- A suitable safety classification scheme has been formulated and applied to structures, systems and components.
- The internal events that could arise for a facility shall be addressed in the safety assessment to demonstrate 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.



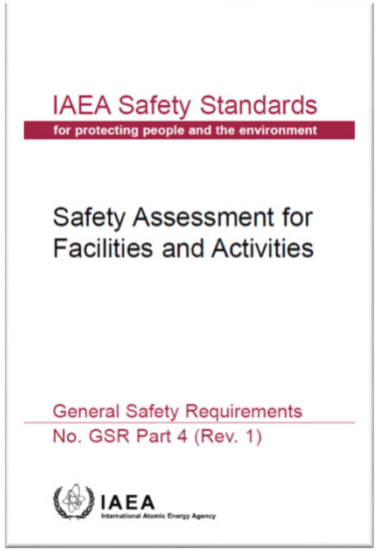
GSR Part 4 Safety Assessment (cont'd)

- 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
- A fail-safe design applied to structures, systems and components as an effective means of detecting failures.



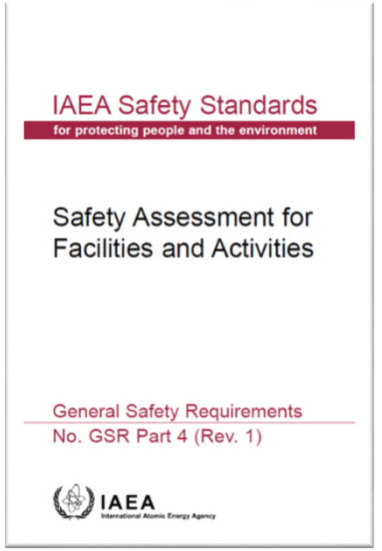
GSR Part 4 Safety Assessment (cont'd)

- 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.
- 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



GSR Part 4 Safety Assessment (cont'd)

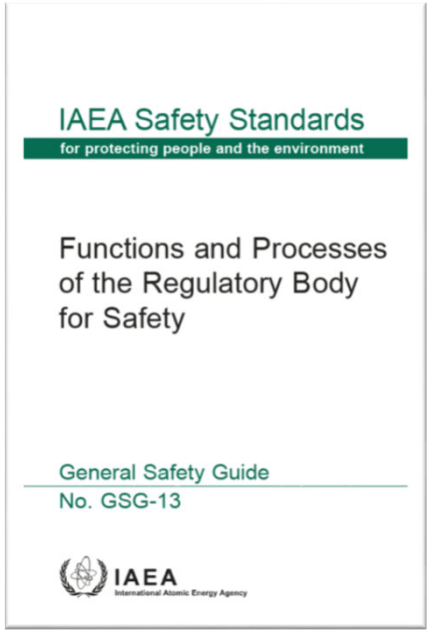
- For sites with multiple facilities or multiple activities, account shall be taken in the safety assessment of the effects of external events on all facilities and activities.
- For facilities on a site that would share resources (whether human resources or material resources) in accident conditions,
- 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

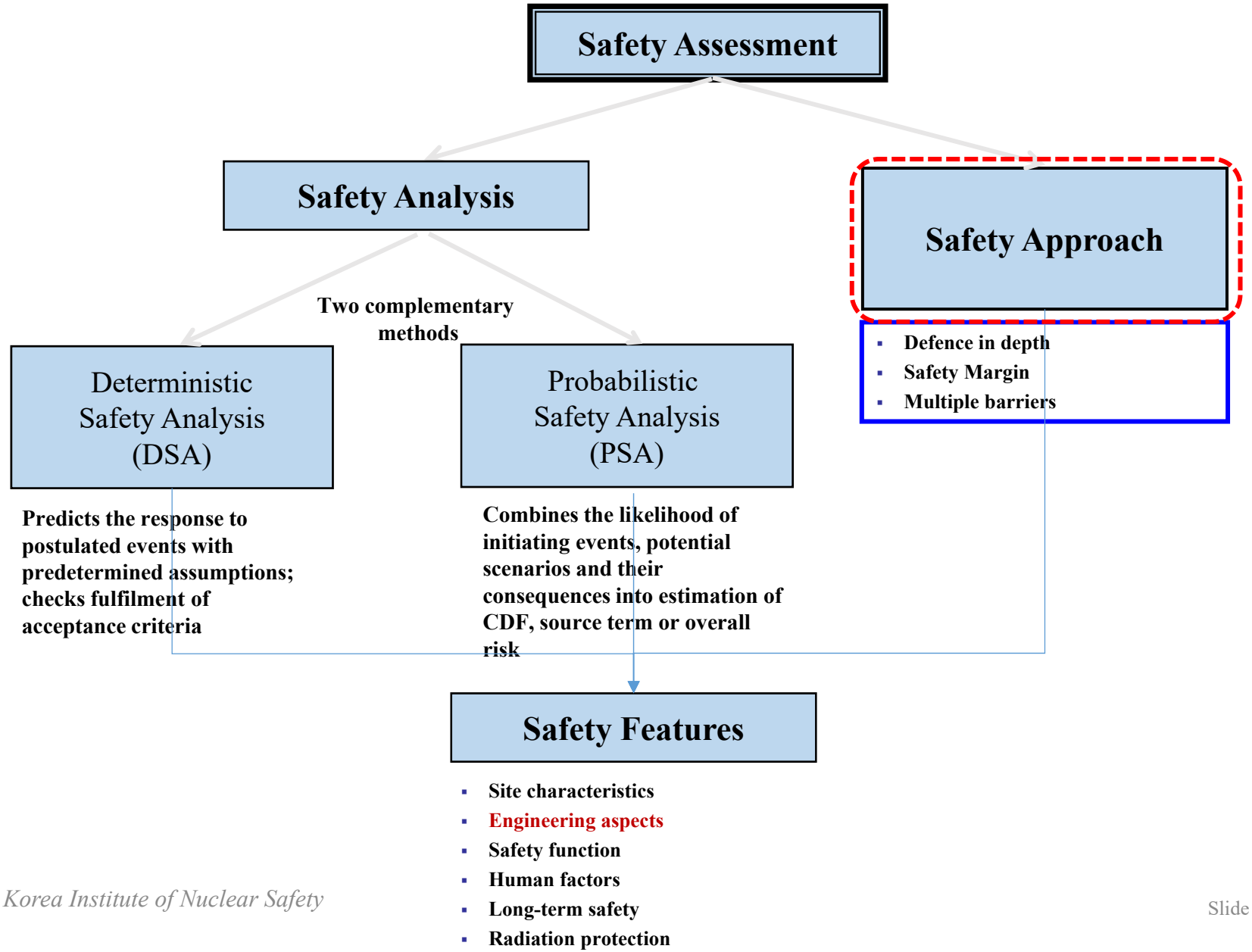
Verification of the safety analysis

- 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 regulatory body should determine whether the authorized party has defined criteria that meet the safety objectives and requirements relating to:
  - Engineering design;
  - Operational and managerial aspects;
  - Normal operation, anticipated operational occurrences and accident conditions.



II. Safety Approach

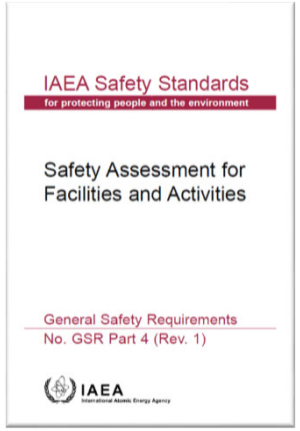
Safety Assessment for Facilities



2. Safety Approach: (1) Defence in depth

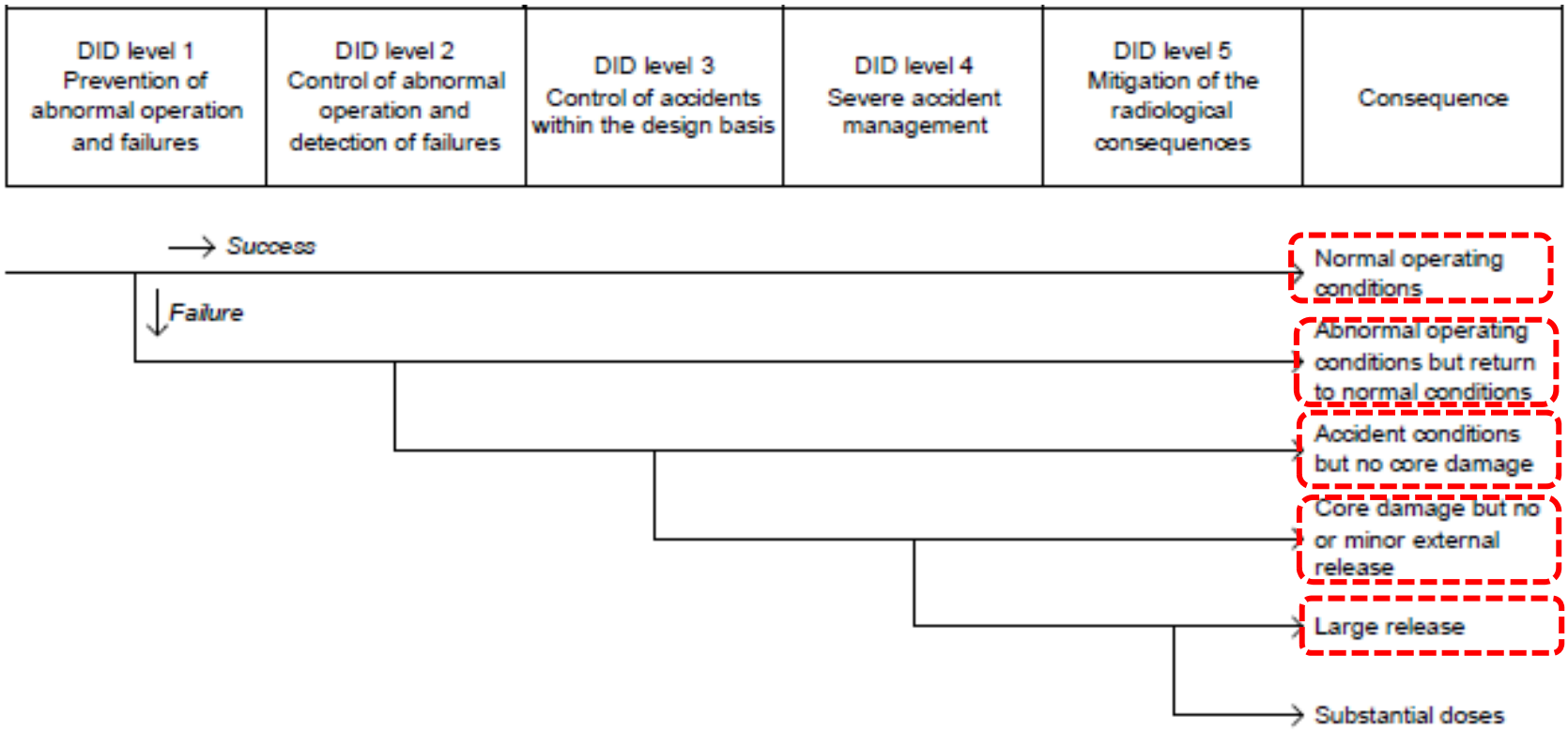
GSR Part 4 Requirement 13: Assessment of defence in depth

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.



- Adequate provisions have been made at each of the levels of defence in depth for the facility:
  - Detect and terminate safety related deviations from normal operation or from its expected evolution in the long term
  - Control accidents within the limits specified in the design;
  - Measures to mitigate the consequences of accidents that exceed design limits;
  - Mitigate radiation risks associated with possible releases of radioactive material.

DiD Event Tree



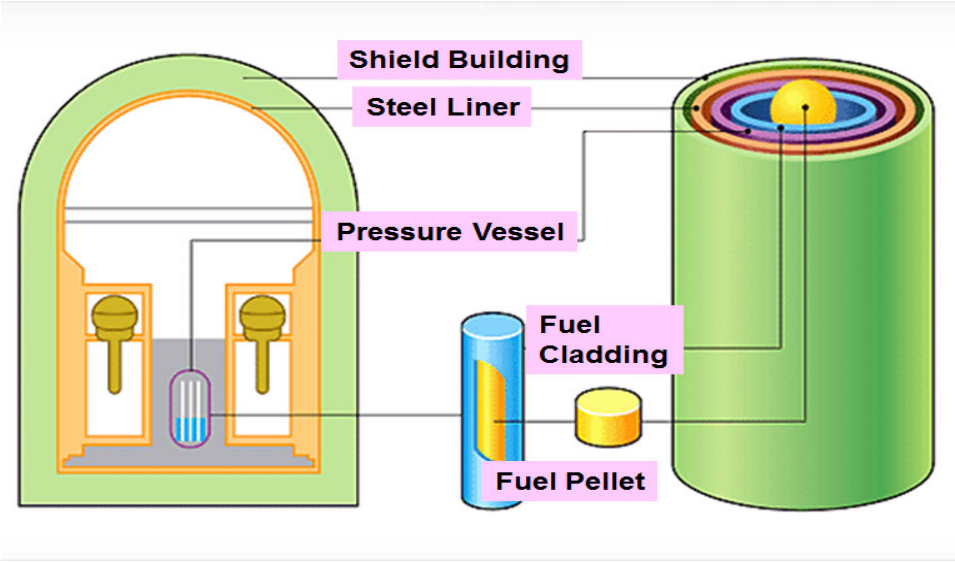
(1) Multiple Physical Barriers of a NPP

- 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)

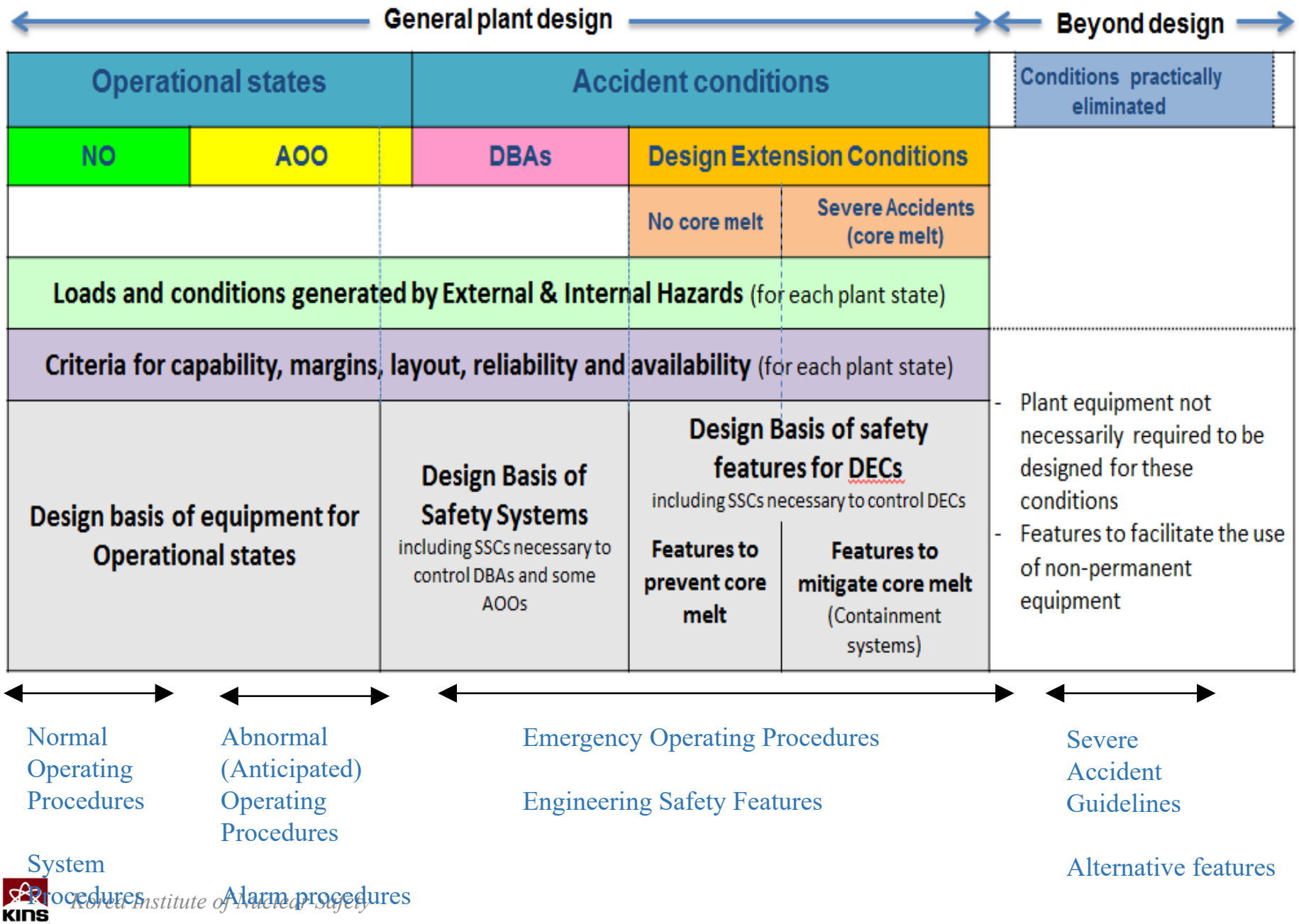
Fuel cladding(ZIRLO)
thickness 0.053cm

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



(2) Levels of Defence in Depth (INSAG-10)

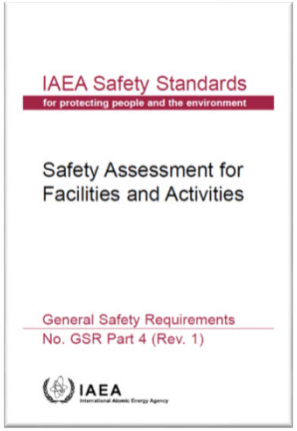
Level	Objective	Essential Means
Level 1	• **Prevention** of abnormal operation and failures.	• Conservative design • High quality in construction operation and operation
Level 2	• **Control** of abnormal operation and **detection** of failures.	• Control, limiting and protection systems and other surveillance 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


General plant design
Beyond design
Operational states
Accident conditions
Conditions practically eliminated
NO
AOO
DBAs
Design Extension Conditions
No core melt
Severe Accidents (core melt)
Loads and conditions generated by External & Internal Hazards (for each plant state)
Criteria for capability, margins, layout, reliability and availability (for each plant state)
Design basis of equipment for Operational states
Design Basis of Safety Systems
including SSCs necessary to control DBAs and some AOOs
Design Basis of safety features for DECs
including SSCs necessary to control DECs
Features to prevent core melt
Features to mitigate core melt
(Containment systems)
- Plant equipment not necessarily required to be designed for these conditions
- Features to facilitate the use of non-permanent equipment
Normal Operating Procedures
System Procedures
Abnormal (Anticipated) Operating Procedures
Alarm procedures
Emergency Operating Procedures
Engineering Safety Features
Severe Accident Guidelines
Alternative features

(2) Safety Margin

GSR Part 4 Defence in depth and safety margins

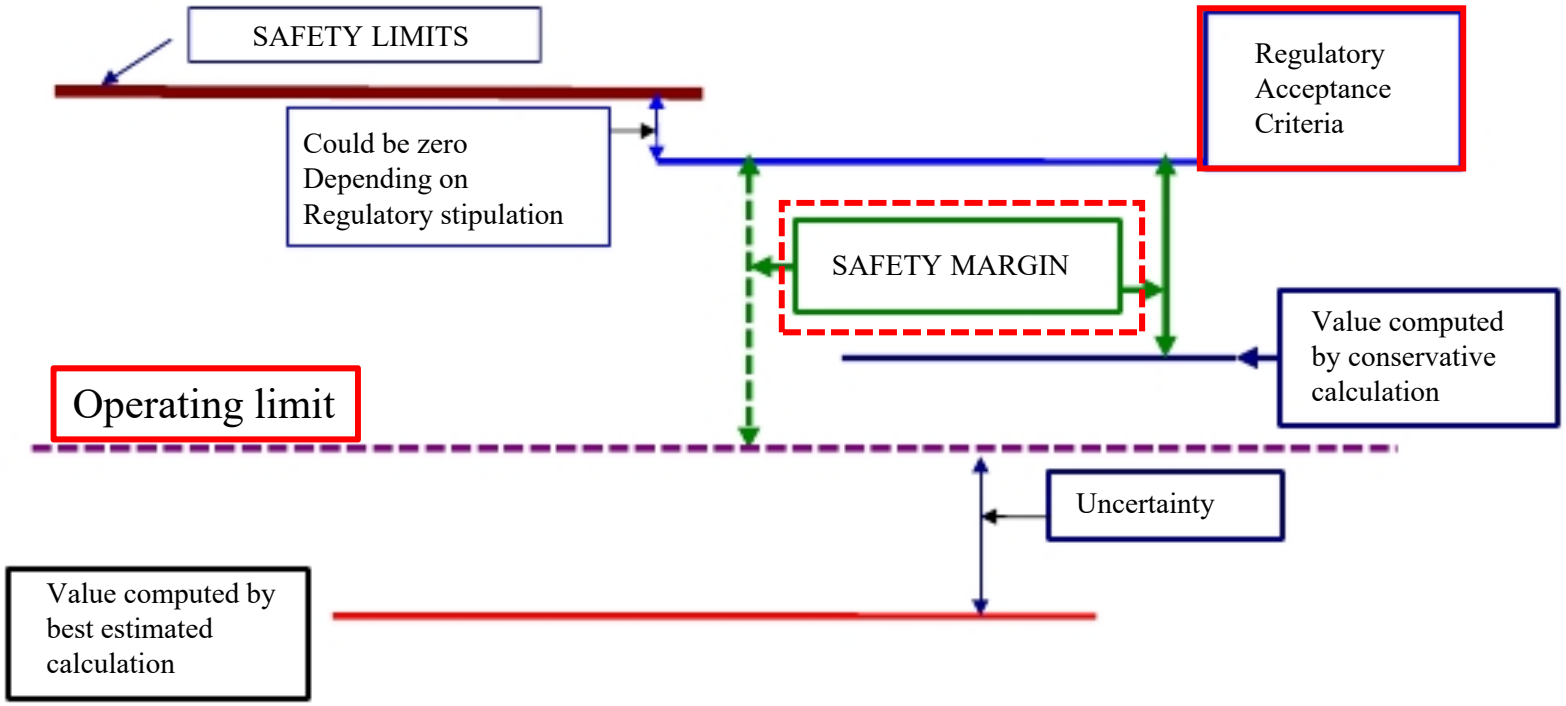
- It shall be determined that there are adequate safety margins in the design and operation of the facility to failure of any structures, systems and components for any of the anticipated operational occurrences or any possible accident conditions.
- The safety assessment shall confirm that there are adequate margins to avoid cliff edge effects that would have unacceptable consequences.



'cliff edge effect' is a 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.

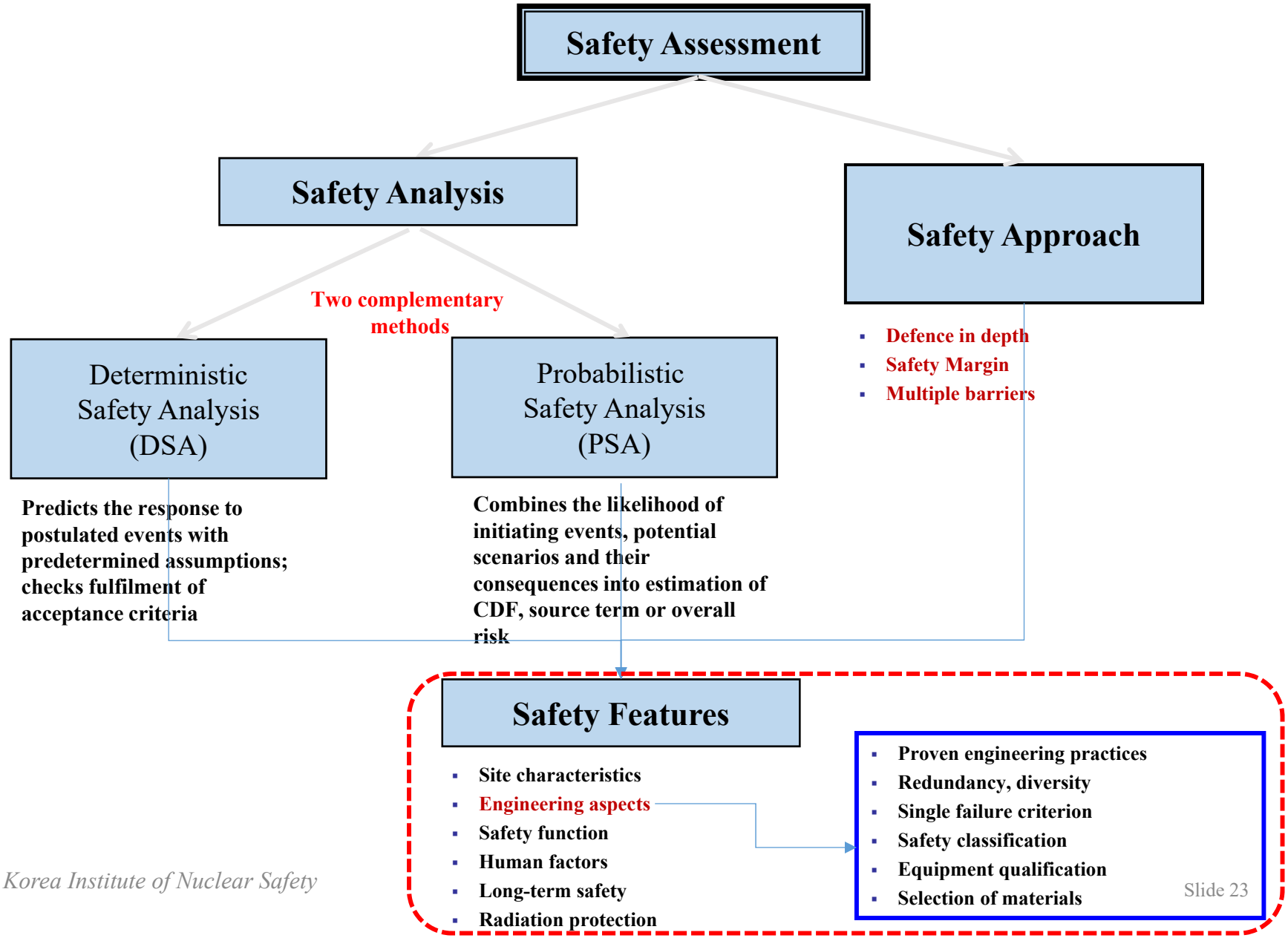
(2) Safety Margins - Definition

- The safety margin is defined as the difference in physical units to the failure of a system or component, and the actual value of that parameter in the plant.



III. Engineering Aspects

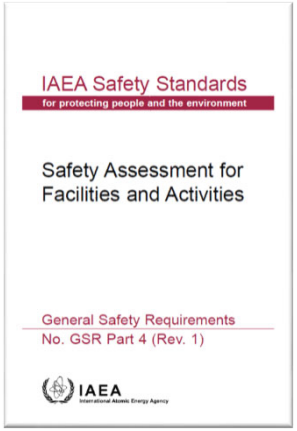
Safety Assessment for Facilities



(1) Proven engineering practices

GSR Part 4 Requirement 10: Assessment of engineering aspects

- 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 by analysis and testing during operation.

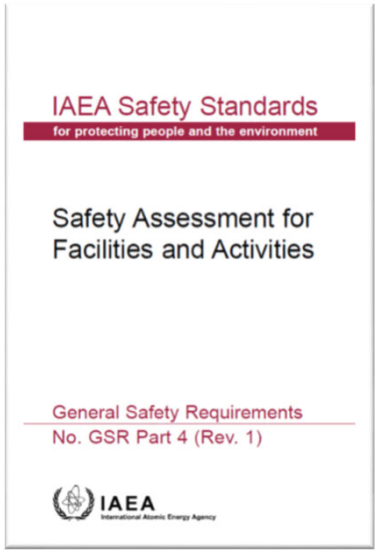


(2) Engineering design rules

- **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.

(3) Safety Function

- Functions that are necessary to be performed to prevent or to mitigate radiological consequences of normal operation, anticipated operational occurrences and accident conditions:
  - control of reactivity,
  - removal of heat from radioactive material (decay heat),
  - confinement of radioactive material



(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 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;
- to remove residual heat(Req. 51) from the reactor core after shutdown, and during and after appropriate operational states and accident conditions;
- to reduce 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.

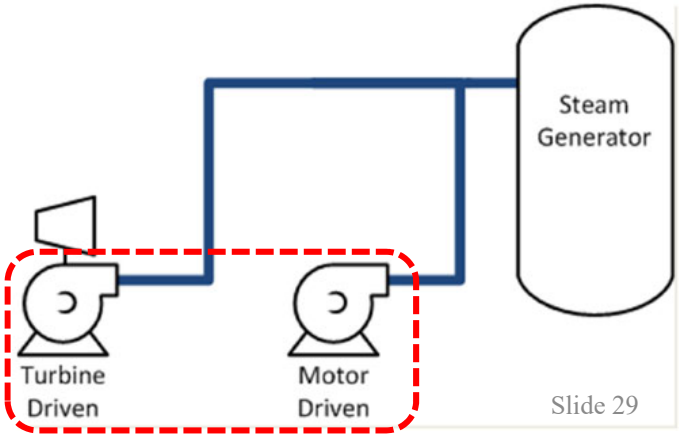
- Structures, systems and components and the barriers that are provided to perform the safety functions have an adequate level of reliability, redundancy, diversity, separation, segregation, independence and equipment qualification, and whether potential vulnerabilities have been identified and eliminated.

(3-1) Diversity

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

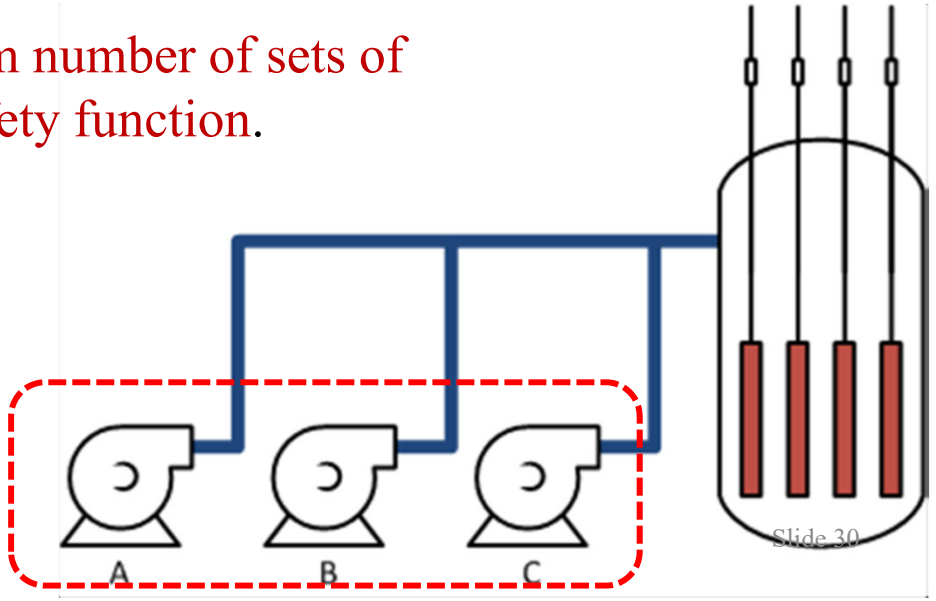
- Diversity is applied to redundant systems or components that perform the same safety function by incorporating different attributes into the systems or components;
  - different principles of operation,
  - different physical variables,
  - different conditions of operation, or
  - production by different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



(3-2) Redundancy

SSR 2/1 Design Requirement 24: Common cause failures

- The design of equipment shall take due account … the concepts of diversity, redundancy, physical separation and functional independence have to be applied to achieve the necessary reliability.
- Redundancy enables failure or unavailability of at least one set of equipment to be tolerated without loss of the function.
  - Use of more than the minimum number of sets of equipment to fulfil a given safety function.



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

SSR 2/1 Design : Requirement 24: Common cause failures

- …. the concepts of diversity, redundancy, physical separation and functional independence have to be applied to achieve the necessary reliability

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 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.

(4) Single failure criterion

SSR-2/1 Requirement 25: Single failure criterion

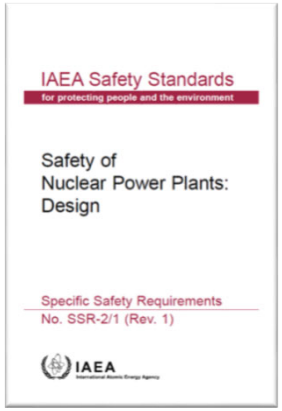
- A failure results in the loss of capability of a system or component to perform its intended safety function.
- The single failure criterion shall be applied to each safety group in the plant design.
  - When applying the single failure criterion to a safety group or safety system, spurious action shall be considered to be one mode of failure.
  - The failure of a passive component also consider 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.

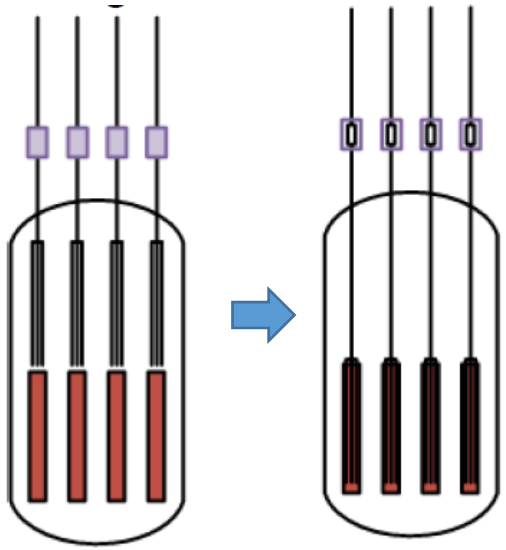
(5) Fail-safe design

SSR-2/1 Requirement 26: Fail-safe design

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

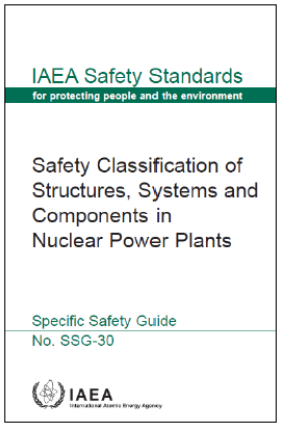
- Systems and components important to safety shall be designed for fail-safe behaviour, as appropriate, so that their failure or the failure of a support feature does not prevent the performance of the intended safety function.





(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 safety significance 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 perform its function



(7) Qualification of items important to safety

- **SSR-2/1 Requirement 30: Qualification of items important to safety**
  - A qualification 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 throughout their design life.

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 basis of the verification of safety by the criteria and proven engineering practices.
- This assessment along with the deterministic and probabilistic approaches practices 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.