Assessment of Engineering Aspects

S. Michael Modro

Joint IAEA-ICTP Essential Knowledge Workshop on Nuclear Power Plant Design Safety-Updated IAEA safety Standards

9-20 October 2017

Trieste, Italy

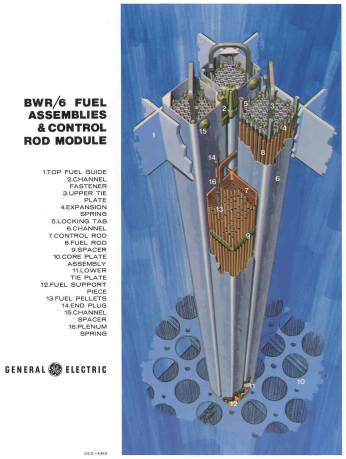
Outline

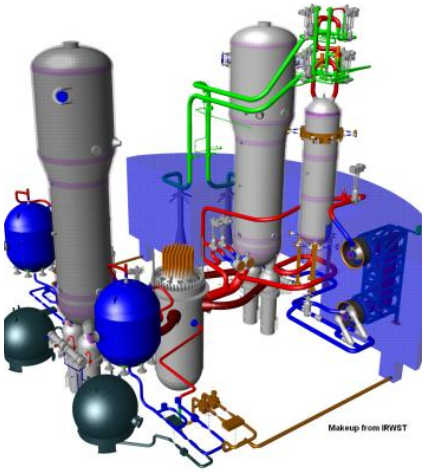
- Safety assessment standards
- Purpose and overall content of safety assessment
- Safety assessment and safety analyses
- Engineering aspects” in the IAEA Safety Standards

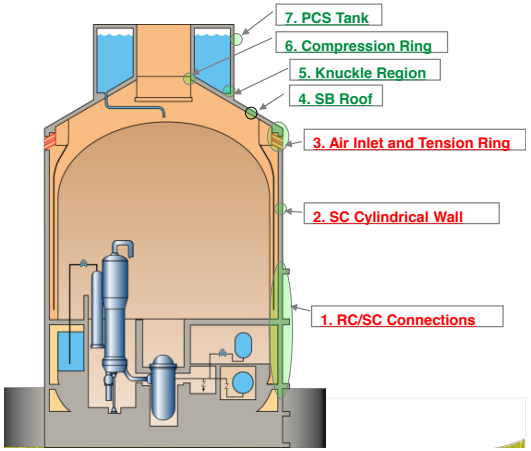
- No clear definition of “engineering aspects important to safety”.
- Common sense: all the engineering and design aspects that assure robust and reliable design (safe).

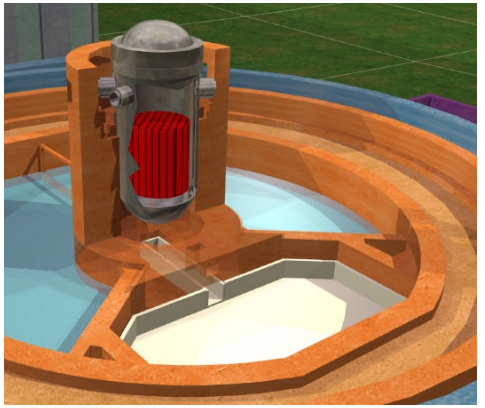
Fundamental safety functions

- Control of reactivity
- Cooling of the core
- Confinement of radioactive materials and control of operational discharges as well as limitation of accidental releases





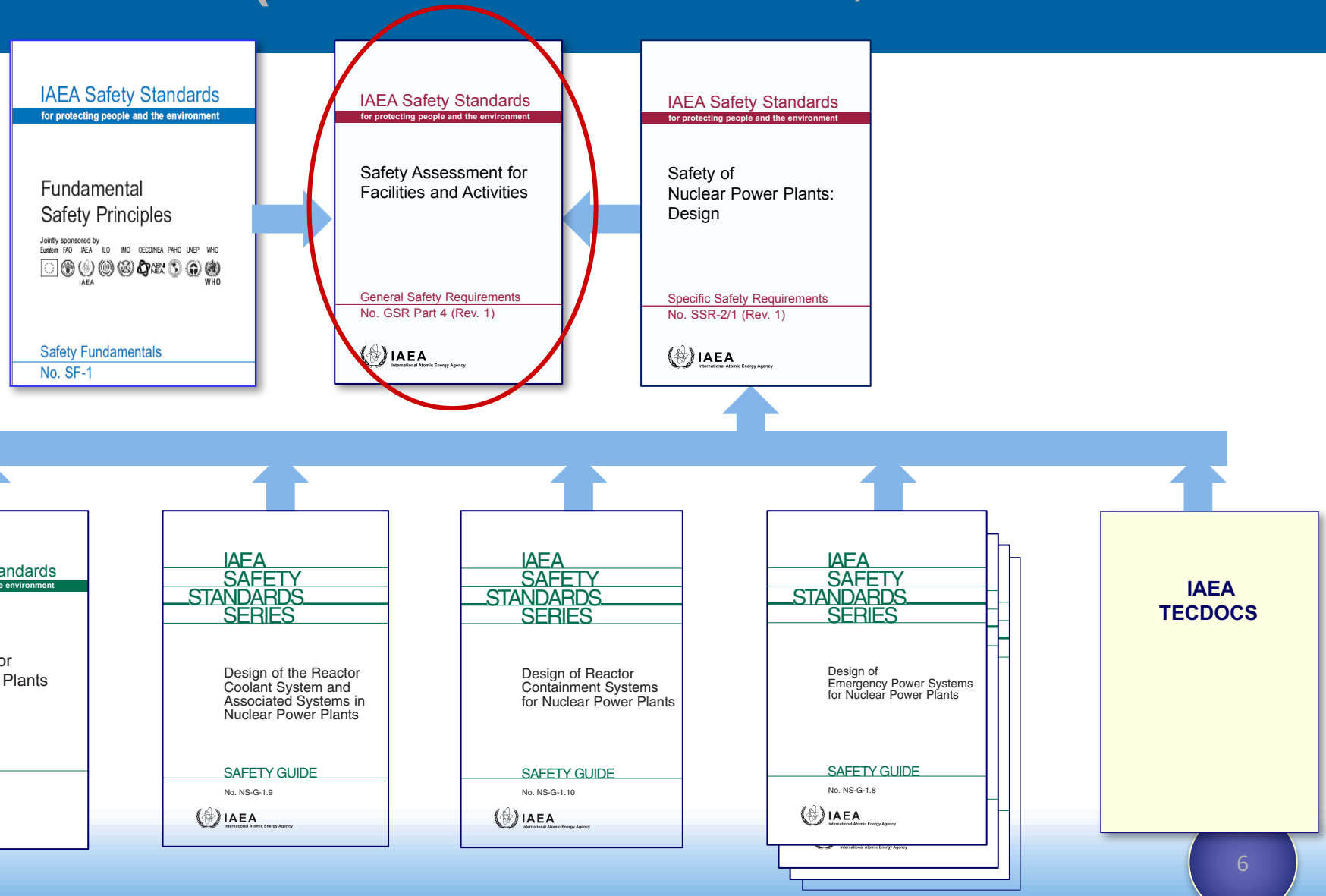




IAEA SAFETY STANDARDS

- Requirements for safety assessment (GSR Part 4) include requirement for assessment of engineering aspects
- To evaluate engineering aspects other standards must be considered as well – most notably the standard addressing requirements for safe design (SSR-2/1 Rev 1)

Relevant IAEA Safety Standards
(AID IN SAFETY ASSESSMENT)



The primary purposes of the safety assessment is to determine whether an adequate level of safety has been achieved.

- The safety assessment has to address all radiation risks that arise from
  - **normal operation,**
  - **anticipated operational occurrences, and**
  - **accident conditions (in which failures or internal or external events have occurred that challenge the safety).**
- The safety assessment for anticipated operational occurrences and accident conditions also has to address **failures** that might occur and the **consequences** of any failures.

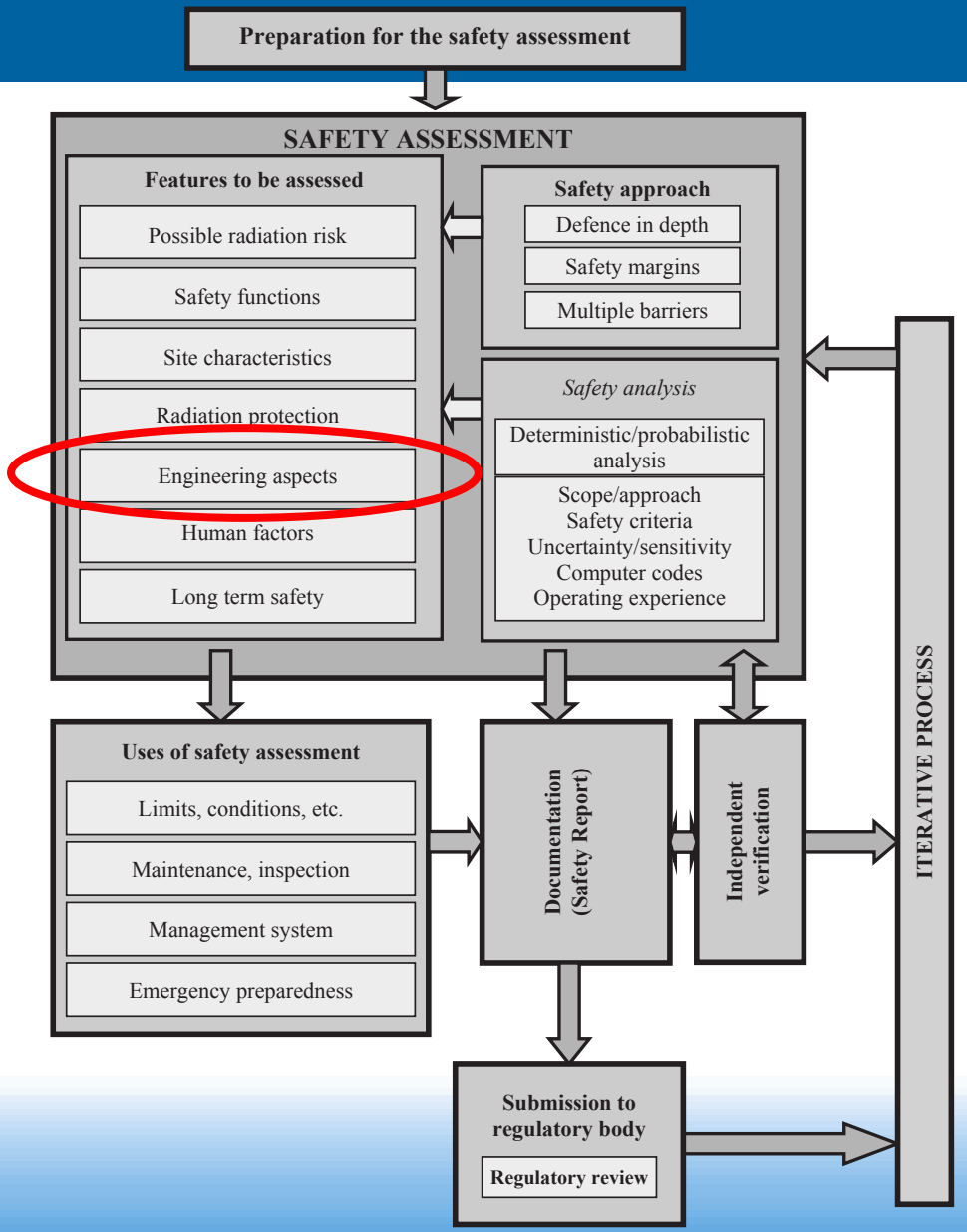
SAFETY ASSESSMENT INCLUDES

- Evaluation whether
  - **Adequate defence in depth** has been provided, as appropriate, through a combination of several layers of protection (i.e. physical barriers, systems to protect the barriers, and administrative procedures) that would have to fail or to be bypassed before there could be any consequences for people or the environment;
  - a facility or activity uses, to the extent reasonable, **structures, systems and components of robust and proven design**;
  - the **procedures and safety measures** that are provided for all normal operational activities, in particular those that are necessary for implementation of the operational limits and conditions, and those that are required in response to anticipated operational occurrences and accidents**, ensure an adequate level of safety**.

SAFETY ASSESSMENT INCLUDES (cont'd)

- **Assessment of the site characteristics** relating to the safety of the facility or activity shall be carried out;
- **All safety functions associated with a facility or activity shall be specified and assessed**;
- **Assessment of the provisions for radiation protection**: whether adequate measures are in place to protect people and the environment from harmful effects of ionizing radiation;
- **Safety analysis**, which consists of a set of different quantitative analyses for evaluating and assessing challenges to safety in various operational states, anticipated operational occurrences and accident conditions, by means of deterministic and also probabilistic methods.

Safety Assessment process (GSR Part 4, Rev 1)



Requirement 10: Assessment of engineering aspects (1/7)

Requirement 10

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.

- **Relevant operating experience**, including results of root cause analysis of operational occurrences, accident conditions and accident precursors where appropriate, shall be taken into account.
- The **design principles that have been applied for the facility are identified** in the safety assessment, **and it shall be determined whether these principles have been met**.
  - The design principles applied will depend on the type of facility but they could give rise to requirements to incorporate defence in depth, multiple barriers to the release of radioactive material, and safety margins, and to provide redundancy, diversity and equipment qualification in the design of safety systems.

Requirement 10: Assessment of engineering aspects (2/7)

- Where **innovative improvements beyond current practices** have been incorporated into the design, it shall be determined 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.
- It shall be determined whether a **suitable safety classification** scheme has been formulated and applied to structures, systems and components.
  - Does the safety classification scheme adequately reflects the **importance to safety of structures, systems and components**, the severity of the consequences of their failure, the requirement or them to be available in anticipated operational occurrences and accident conditions?
  - Are the systems and components adequately qualified?
  - Does the scheme identifies the **appropriate industry codes and standards** and the **regulatory requirements** to be applied in the design, manufacturing, construction and inspection of engineered features, in the development of procedures and in the management system for the facility or activity.

Requirement 10: Assessment of engineering aspects (3/7)

External Events

- The **external events** that could arise for a facility or activity shall be addressed in the safety assessment, and it shall be determined whether an **adequate level of protection against their consequences is provided.**
  - This could include natural external events, such as extreme weather conditions, and human induced events, such as aircraft crashes, depending on the possible radiation risks associated with the facility or activity.
- The **magnitude of the external events** that the facility is required to be able to withstand shall be **established** for each type of external event on the basis of historical data for the site for natural external events and a survey of the site and the surrounding area for human induced events.
- Where appropriate, the safety assessment shall demonstrate that **the design is adequately conservative** so that **margins are available to withstand external events more severe than those selected for the design basis**.

Requirement 10: Assessment of engineering aspects (4/7)

Internal Events

- 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 that were taken into account explicitly in the design of the facility.
  - consideration of specific loads and load combinations,
  - environmental conditions (e.g. temperature, pressure, humidity and radiation levels) imposed on structures and components as a result of internal events, such as pipe breaks, impingement forces, internal flooding and spraying, internal missiles, load drop, internal explosions and fire.

Requirement 10: Assessment of engineering aspects (5/7)

It shall be determined 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 that were taken into account explicitly in the design of the facility or activity.
- **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.
- 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. This shall include the assessment of ageing management programmes for nuclear facilities.

Requirement 10: Assessment of engineering aspects (6/7)

It shall be determined 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 that were taken into account in the design, and in conditions that may arise as a result of external events that were taken into account in the design.
- 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, including the possibility of concurrent events affecting different facilities and activities, and of the potential hazards presented by each facility or activity to the others.

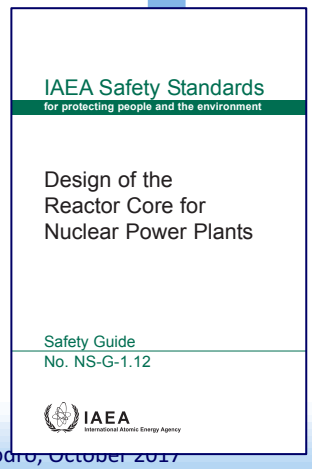
Requirement 10: Assessment of engineering aspects (7/7)

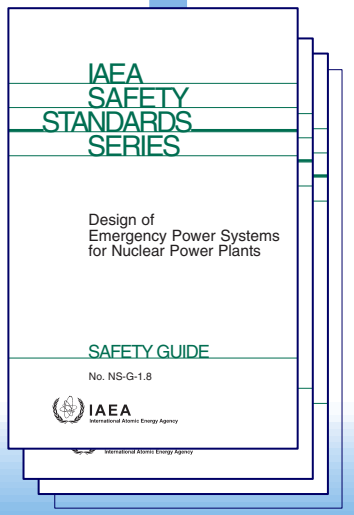
- **For facilities** on a site **that would share resources** (whether human resources or material resources) in accident conditions, the safety assessment shall **demonstrate that the required safety functions can be fulfilled at each facility in accident conditions**.
- The **provisions made for the decommissioning and dismantling** of a facility or for the closure of a disposal facility for radioactive waste shall be specified, and it shall be determined in the safety assessment whether they are adequate.

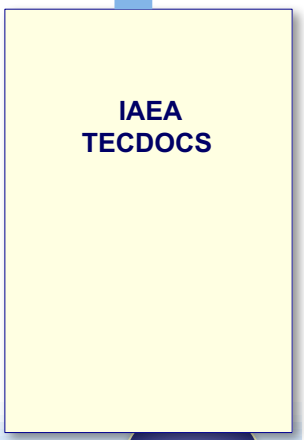
Examples of Engineering Design Rules for SSCs

	CHALLENGES (examples)	DESIGN SOLUTIONS (examples)
CAPABILITY	Failure to perform safety function adequately	• Appropriate code selection • Conservative margins • Material selection • Design qualification
DEPENDABILITY	Effect of : • Single failure • Common cause failure • Errors in design, construction, maintenance and operation • Failure of supporting systems	• Appropriate code selection • Fail-safe design • Reliability/availability • Diversity • Redundancy • Independence • Maintainability • Testability • Material selection • Design qualification • Surveillance methodology
ROBUSTNESS	Effect of : • Internal hazards • External hazards • Harsh and moderate environmental conditions • Induced loads	• Appropriate code selection • Fail-safe design • Material selection • Seismic and environmental qualification • Diversity • Separation • Independence • Maintainability • Testability

Relevant IAEA Safety Standards

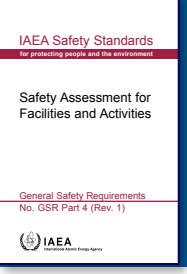






SSR-2/1 Rev 1
4. PRINCIPALTECHNICALREQUIREMENTS

- Requirement 4: Fundamental safety functions (4.1–4.2)
- Requirement 5: Radiation protection in design (4.3–4.4)
- Requirement 6: Design for a nuclear power plant (4.5–4.8)
- Requirement 7: Application of defence in depth (4.9–4.13A)
- Requirement 8: Interfaces of safety with security and safeguards
- Requirement 9: Proven engineering practices (4.14–4.16)
- Requirement 10: Safety assessment (4.17–4.18)
- Requirement 11: Provision for construction (4.19)
- Requirement 12: Features to facilitate radioactive waste management and decommissioning (4.20)



SSR-2/1 Rev 1
5. GENERALPLANTDESIGN

Design basis

- Requirement 13: Categories of plant states (5.1–5.2)
- Requirement 14: Design basis for items important to safety (5.3)
- Requirement 15: Design limits (5.4)
- Requirement 16: Postulated initiating events (5.5–5.15)
- Requirement 17: Internal and external hazards (5.15A–5.22)
- Requirement 18: Engineering design rules (5.23)
- Requirement 19: Design basis accidents (5.24–5.26)
- Requirement 20: Design extension conditions (5.27–5.32)
- Requirement 21: Physical separation and independence of safety systems (5.33)
- Requirement 22: Safety classification (5.34–5.36)
- Requirement 23: Reliability of items important to safety (5.37–5.38)
- Requirement 24: Common cause failures
- Requirement 25: Single failure criterion (5.39–5.40)
- Requirement 26: Fail-safe design (5.41)
- Requirement 27: Support service systems (5.42–5.43)
- Requirement 28: Operational limits and conditions for safe operation (5.44)

SSR-2/1 Rev 1
5. GENERALPLANTDESIGN cont'd

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 (5.45–5.47)
- Requirement 30: Qualification of items important to safety (5.48–5.50)
- Requirement 31: Ageing management (5.51–5.52)

Human factors

- Requirement 32: Design for optimal operator performance (5.53–5.62)

Other design considerations

- Requirement 33: Safety systems, and safety features for design extension conditions, of units of a multiple unit nuclear power plant (5.63)
- Requirement 34: Systems containing fissile material or radioactive material
- Requirement 35: Nuclear power plants used for cogeneration of heat and power, heat generation or desalination
- Requirement 36: Escape routes from the plant (5.64–5.65)
- Requirement 37: Communication systems at the plant (5.66–5.67)
- Requirement 38: Control of access to the plant (5.68)

SSR-2/1 Rev 1
5. GENERALPLANTDESIGN cont'd

- Requirement 39: Prevention of unauthorized access to, or interference with, items important to safety
- Requirement 40: Prevention of harmful interactions of systems important to safety (5.69–5.70)
- Requirement 41: Interactions between the electrical power grid and the plant

Safety analysis

- Requirement 42: Safety analysis of the plant design (5.71–5.76)

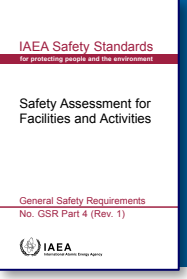
SSR-2/1 Rev 1
6. DESIGN OF SPECIFIC PLANT SYSTEMS

Reactor core and associated features

- Requirement 43: Performance of fuel elements and assemblies (6.1–6.3)
- Requirement 44: Structural capability of the reactor core
- Requirement 45: Control of the reactor core (6.4–6.6)
- Requirement 46: Reactor shutdown (6.7–6.12)

Reactor coolant systems

- Requirement 47: Design of reactor coolant systems (6.13–6.16)
- Requirement 48: Overpressure protection of the reactor coolant pressure boundary
- Requirement 49: Inventory of reactor coolant
- Requirement 50: Cleanup of reactor coolant (6.17)
- Requirement 51: Removal of residual heat from the reactor core
- Requirement 52: Emergency cooling of the reactor core (6.18–6.19)
- Requirement 53: Heat transfer to an ultimate heat sink(6.19A–6.19B)



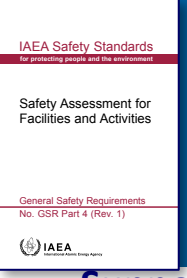
SSR-2/1 Rev 1
6. DESIGN OF SPECIFIC PLANT SYSTEMS cont'd

Containment structure and containment system

- Requirement 54: Containment system for the reactor
- Requirement 55: Control of radioactive releases from the containment (6.20–6.21)
- Requirement 56: Isolation of the containment (6.22–6.24)
- Requirement 57: Access to the containment (6.25–6.26)
- Requirement 58: Control of containment conditions (6.27–6.30)

Instrumentation and control systems

- Requirement 59: Provision of instrumentation (6.31)
- Requirement 60: Control systems
- Requirement 61: Protection system (6.32–6.33)
- Requirement 62: Reliability and testability of instrumentation and control systems (6.34–6.36)
- Requirement 63: Use of computer based equipment in systems important to safety (6.37)
- Requirement 64: Separation of protection systems and control systems (6.38)
- Requirement 65: Control room (6.39–6.40A)
- Requirement 66: Supplementary control room (6.41)
- Requirement 67: Emergency response facilities on the site (6.42)Emergency power supply
- Requirement 68: Design for withstanding the loss of off-site power (6.43–6.45A)



SSR-2/1 Rev 1
6. DESIGN OF SPECIFIC PLANT SYSTEMS cont'd

Supporting systems and auxiliary systems

- Requirement 69: Performance of supporting systems and auxiliary systems
- Requirement 70: Heat transport systems (6.46)
- Requirement 71: Process sampling systems and post-accident sampling systems (6.47)
- Requirement 72: Compressed air systems
- Requirement 73: Air conditioning systems and ventilation systems (6.48–6.49)
- Requirement 74: Fire protection systems (6.50–6.54)
- Requirement 75: Lighting systems
- Requirement 76: Overhead lifting equipment (6.55)

Other power conversion systems

- Requirement 77: Steam supply system, feedwater system and turbine generators (6.56–6.58)

Treatment of radioactive effluents and radioactive waste

- Requirement 78: Systems for treatment and control of waste (6.59–6.60)
- Requirement 79: Systems for treatment and control of effluents (6.61–6.63)

Fuel handling and storage systems

- Requirement 80: Fuel handling and storage systems (6.64–6.68A)

Radiation protection

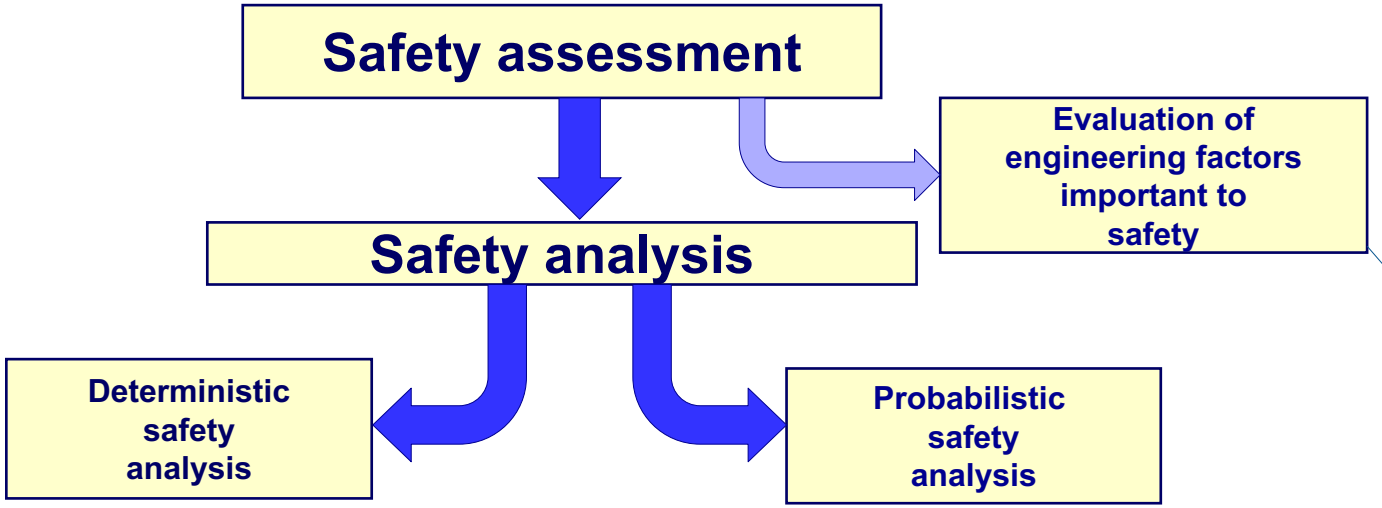
- Requirement 81: Design for radiation protection (6.69–6.76)
- Requirement 82: Means of radiation monitoring (6.77–6.84)

Concluding remark

- Designing structures, systems and components according to the requirements established for engineering aspects provides a robust design (strong prevention of failures and effective protection of people)
- The assessment of engineering aspects ensures, together with the safety analysis, that all the acceptance criteria are met and the plant performs as intended from a safety point of view
- The IAEA Safety Standards provide excellent base for review and assessment of the a NPP design for its robustness and safety

…Thank you for your attention

Safety assessment and safety analysis



- Proven engineering practices
- Defence in depth
- Radiation protection
- Protection against external hazards
- Combination of loads
- Selection of materials
- Single failure criterion
- Redundancy, diversity
- Equipment qualification
- Ageing
- Man-machine interface
- …..

Two quantitative and complementary safety assessment methods

Deterministic safety analysis
= analytical evaluations of physical phenomena (plant performance) for all plant states.

Probabilistic safety analysis
= systematic and comprehensive methodology to evaluate risks.

SF-1: “Safety has to be assessed for all facilities and activities”