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

Trieste,12-23 October 2015

Introduction to the Assessment of Engineering Aspects

Marco Gasparini

IAEA
International Atomic Energy Agency

Outline

- “Engineering aspects” in the IAEA Safety Standards
- Safety assessment and safety analysis
- Engineering aspects and Safety Analysis Report
- Evaluation of engineering aspects

Main references: IAEA Safety Standards and Glossary of Terms

IAEA

The term "engineering aspects" in the IAEA safety standards

- The term “Engineering aspects important to safety” is used in NS-G-1.2 Safety Assessment and verification for NPP (2001)
- Term not used in SSR-2/1 – Safety of Nuclear Power Plant: Design (2012) – although requirements are given for each aspect
- The term “Engineering aspects” is used in GSR-Part 4 Safety Assessment for Facilities and Activities and general requirements are given for their assessment

IAEA

IAEA Safety Fundamentals (2006)

Safety Objective

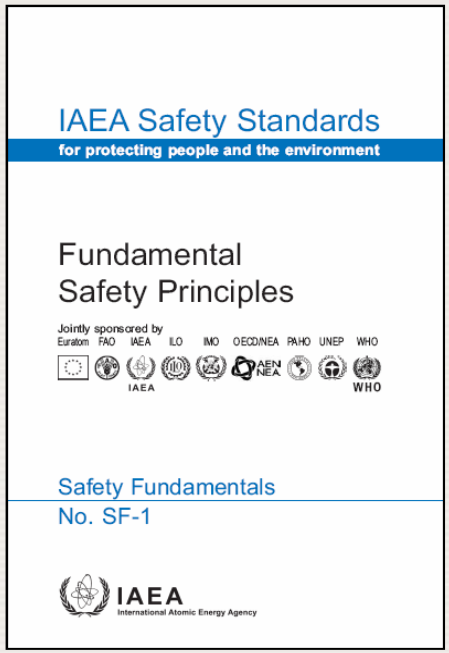
To protect people and the environment from harmful effects of ionizing radiation

Responsibility for Safety

Role of Government

Leadership and Management for Safety

Justification of Facilities and Activities



Optimization of Protection

Limitation of Risks to Individuals

Protective Actions to Reduce Existing Or Unregulated Radiation Risks

Emergency Preparedness and Response

Prevention of Accidents

Protection of Present and Future Generations

IAEA

Principle 8: Prevention of accidents

- 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”
    - Consecutive and independent levels of protection

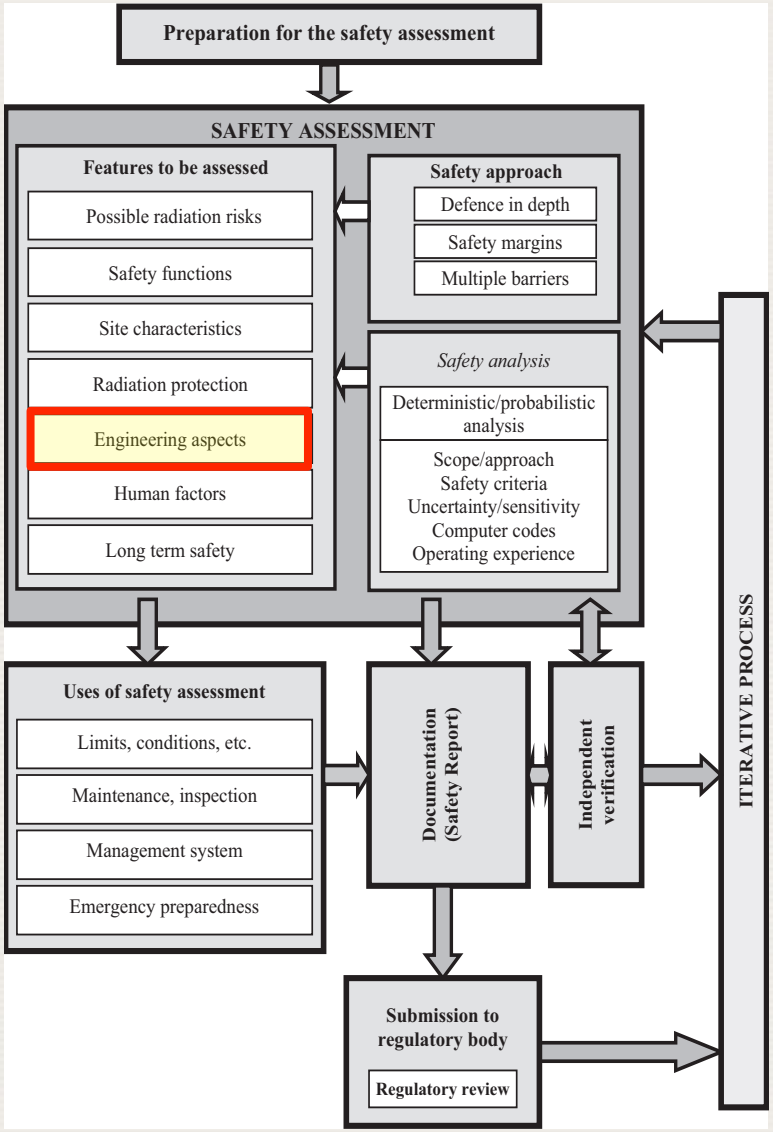
IAEA

Primary means to achieve defence in depth

- An effective management system, strong commitment to safety and strong safety culture
- Adequate site selection and the incorporation of good design and engineering features providing safety margins, diversity and redundancy
- Design, technology and materials of high quality and reliability
- Control, limiting and protection systems and surveillance features
- Appropriate combination of inherent and engineered safety features
- Comprehensive operational procedures and practices as well as accident management procedures

IAEA

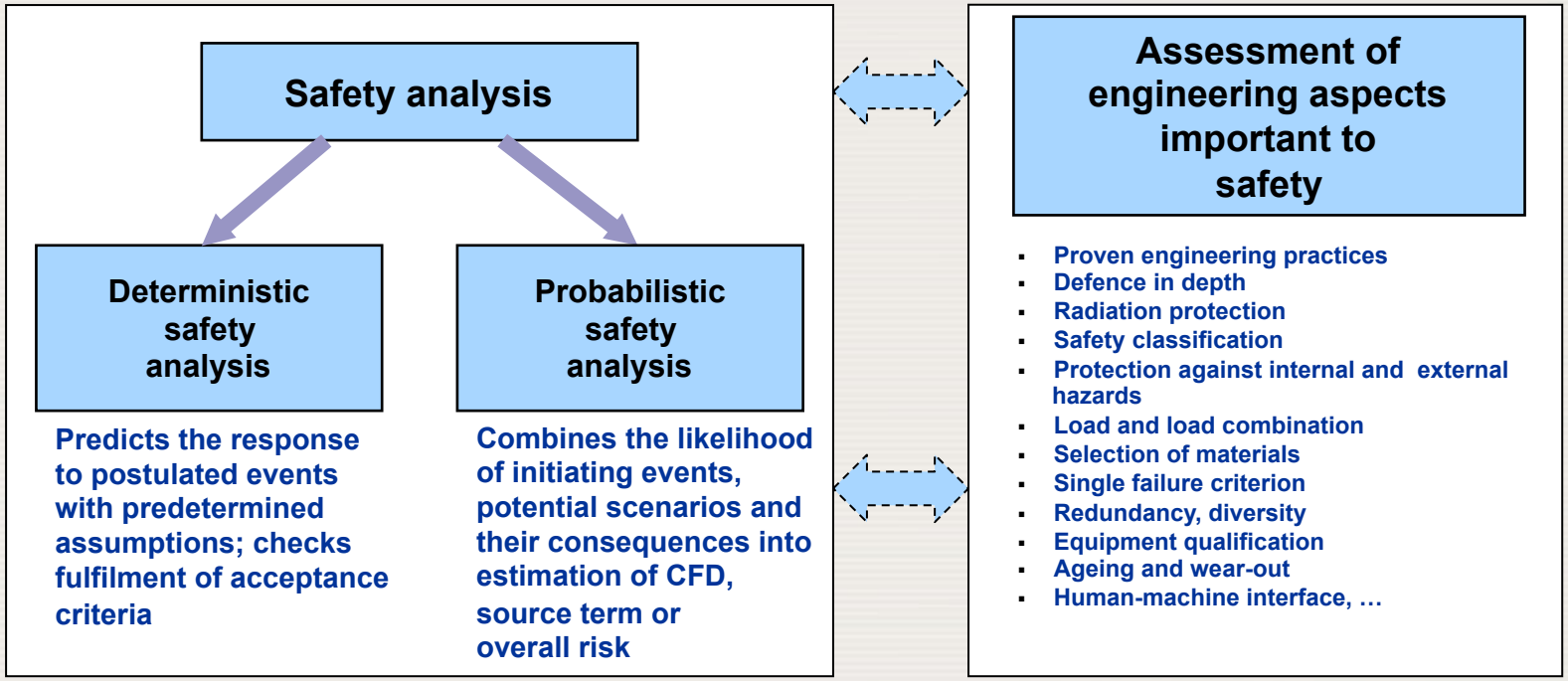
Overview of the safety assessment process (GSR Part 4)



IAEA

Safety assessment and safety analysis

SAFETY ASSESSMENT (NS-G-1.2)

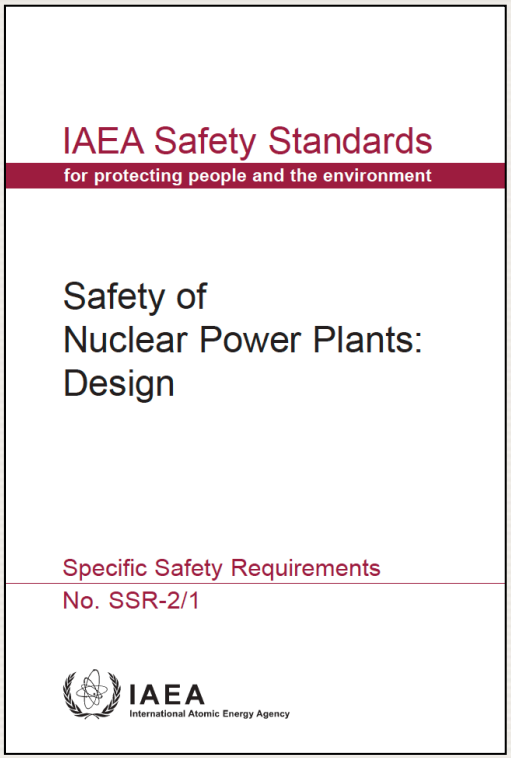


While the assessment of engineering aspects important to safety may not be explicitly addressed in the safety analysis, it constitutes a relevant part of the safety assessment. For some of these aspects, no well-defined acceptance criteria are available and therefore the assessment of the compliance with the safety requirements is based on good engineering judgement.

IAEA

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

SSR-2/1 (revision of NS-R-1) has been published on Feb 2012

IAEA

Design and assessment of engineering aspects

- 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

GSR Part 4 - 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.

Engineering aspects addressed under Requirement 10:

- Relevant operating experience.
- Appropriate programme of research, analysis and testing for innovative design features.
- Suitable safety classification scheme.
- Appropriate industry codes, standards and the regulatory requirements in the
  - design, manufacturing and construction
  - Inspection of engineered features,
  - management system for the facility or activity.
- External events and adequate level of protection against their consequences.

IAEA

GSR Part 4-Requirement 10: Assessment of engineering aspects (cont'd)

- Internal events,
- Use of suitable materials
- Preference to a fail-safe design
- Time related aspects, such as ageing and wear out , or life limiting factors, such as cumulative fatigue, embrittlement, corrosion, chemical decomposition and radiation induced damage, and aging management.
- Qualification of equipment essential to safety to a sufficiently high level.
- Provisions for the decommissioning and dismantling.

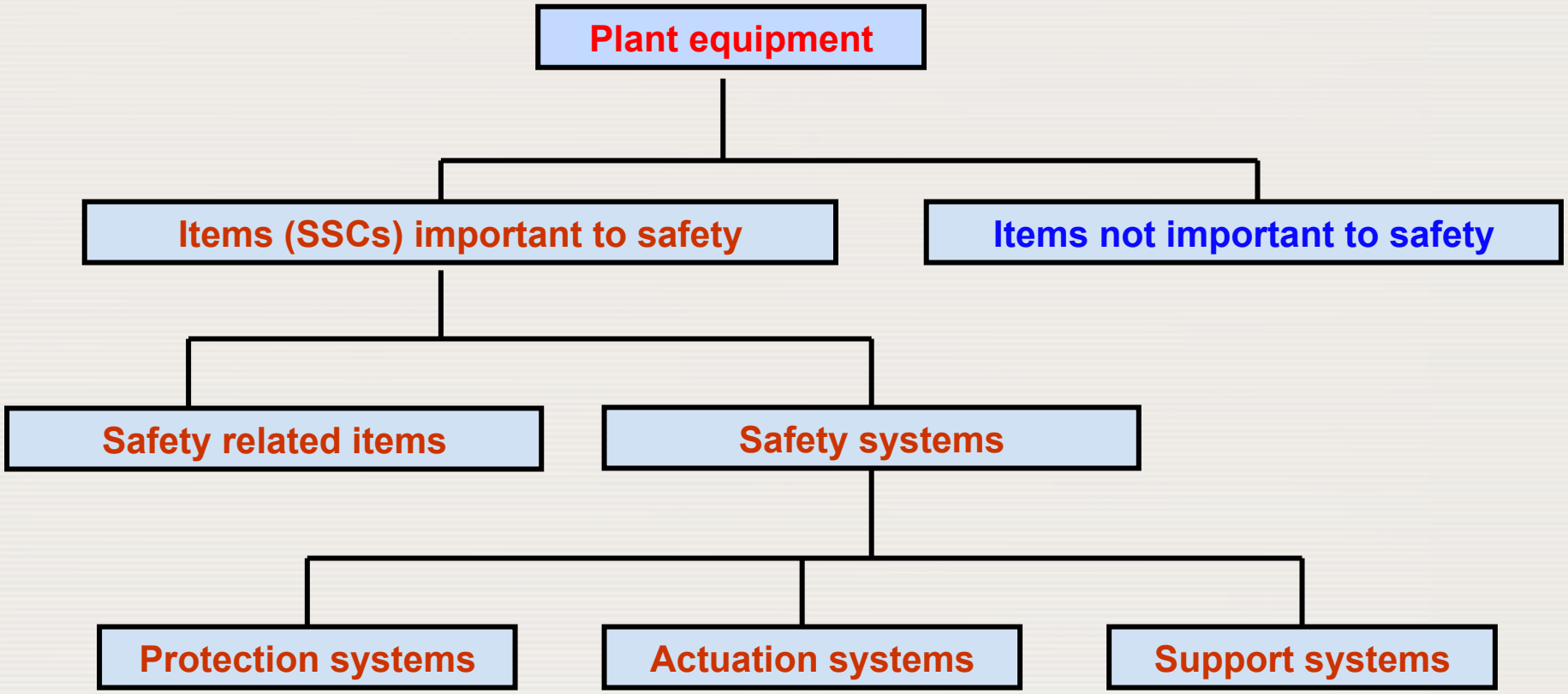
IAEA

Other aspects important to safety

- Defence in depth.
- Radiation protection and acceptance criteria.
- Human factors.
- In-service testing, maintenance, repair inspection and monitoring.
- The application of diversity, redundancy and independence.

IAEA

Plant Equipment categories

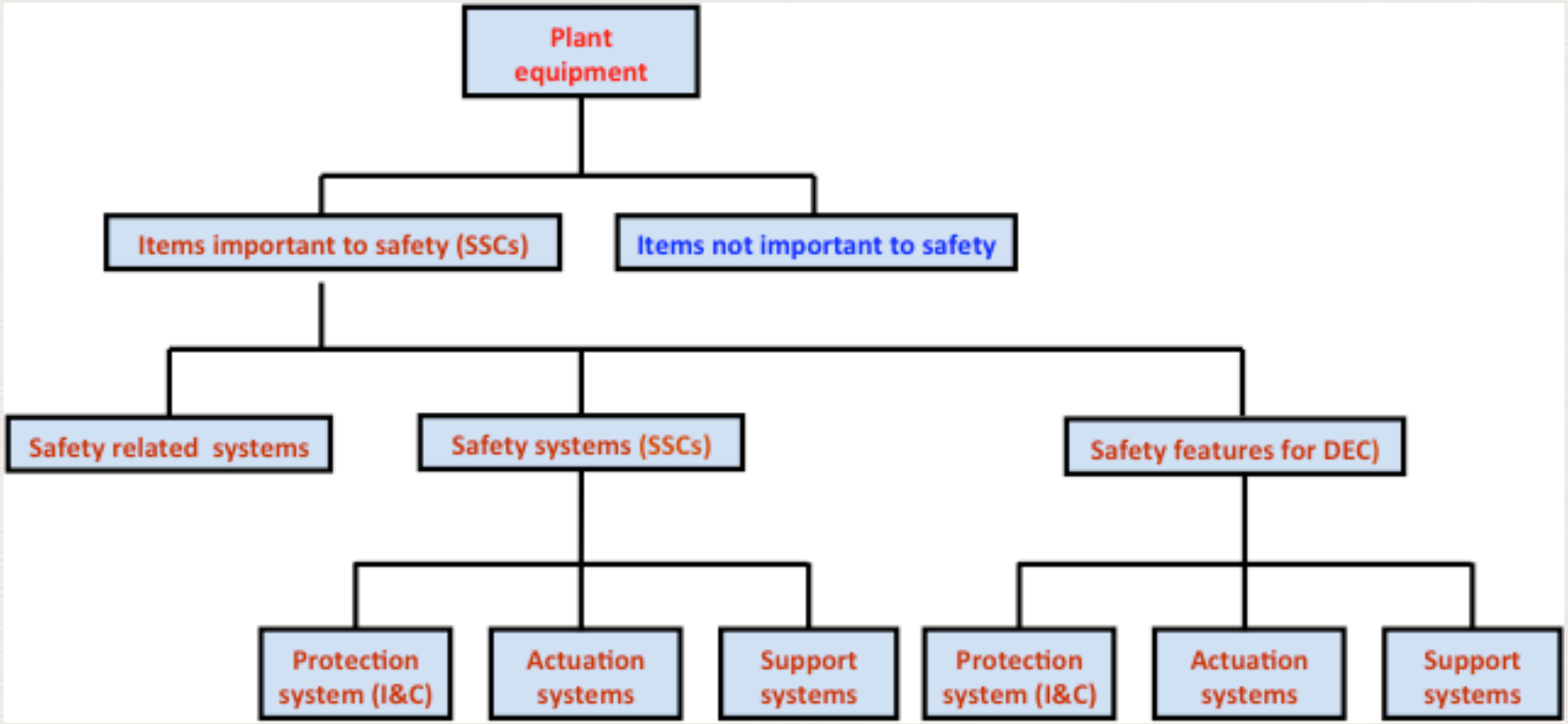


* SSCs = Systems, structures and components

(after IAEA Glossary)

IAEA

Plant equipment (Structures, systems and components)



IAEA

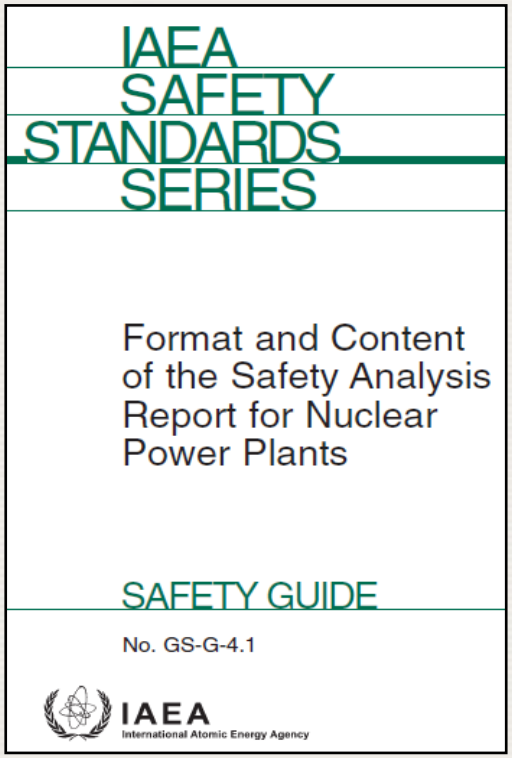
Engineering aspects and Safety Analysis Report

The demonstration that the NPP uses structures, systems and components of robust and proven design has to be provided in The Safety Analysis Report.

Safety Analysis Report (SAR)

- Engineering aspects important to safety and safety analysis are addressed in the SAR for the NPP

- **Chapter I: Introduction**
- **Chapter II: General plant description**
- **Chapter III: Management of safety**
- **Chapter IV: Site evaluation**
- **Chapter V: General design aspects**
- **Chapter VI: Description and conformance to the design**
- **of plant systems**
- **Chapter VII: Safety analyses**
- **Chapter VIII: Commissioning**
- **Chapter IX: Operational aspects**
- **Chapter X: Operational limits and conditions**
- **Chapter XI: Radiation protection**
- **Chapter XII: Emergency preparedness**
- **Chapter XIII: Environmental aspects**
- **Chapter XIV: Radioactive waste management**
- **Chapter XV: Decommissioning and end of life aspects**



IAEA

Comparison of SAR formats

RG-1. 70 (US-NRC)	GS-G-4.1 (IAEA)
1. Introduction and general description of the plant	1. Introduction
2. Site Characteristics	2. General Plant Description
3. Design of Structures, Components, Equipment and Systems	3. Management of Safety
4. Reactor	4. Site Evaluation
5. RCS and Connected Systems	5. General Design Aspects
6. Engineered Safety Features	6. Description and conformance to the design of plant systems
7. Instrumentation and Controls	7. Safety analyses
8. Electric Power	8. Commissioning
9. Auxiliary Systems	9. Operational aspects
10. Steam and Power Conversion	10. Operational limits and conditions
11. Radioactive Waste Management	11. Radiation protection
12. Radiation Protection	12. Emergency preparedness
13. Conduct of Operations	13. Environmental aspects
14. Initial Test Program	14. Radioactive waste management
15. Accident Analyses	15. Decommissioning and end of life aspects
16. Technical Specifications	The NRC guide is more detailed

Evolution of US-NRC-RG 1.70

- **Regulatory Guide 1.206 - Combined License Applications for Nuclear Power Plants, June 2007, applicable for new LWRs**
- **RG 1.206 includes two additional chapters**
  - 18. Human Factors Engineering; it shall be demonstrated that acceptable HFE practices and guidelines are incorporated into the plant's design.
  - 19. Probabilistic Risk Assessment and Severe Accidents; contains summary of design-specific or plant-specific PRA as well as deterministic evaluation of design features for the prevention or mitigation of severe accidents.
- Detailed contents of the SAR can be verified for all chapters, including 18 and 19, using **US NRC Standard Review Plan, NUREG 0800** (constantly updated)

IAEA

Proven engineering practice

SSR-2/1 Req. 9: Proven engineering practices

Items important to safety shall be designed in accordance with relevant national and international codes and standards.

- Items important to safety shall preferably be of a design that has previously proven in equivalent applications, and if not, shall be of high quality and of a technology that has been qualified and tested.
- National and international codes and standards that are used shall be identified and evaluated to determine, their applicability, adequacy and sufficiency.
- Where an unproven design or feature is introduced, safety shall be demonstrated by means of appropriate research programmes, performance tests, operating experience from other relevant applications.

IAEA

Defence in depth

SSR-2/1 Req. 7: Defence in depth

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

- The engineering aspects impact all level of defence in depth, however they are particularly relevant to the **1st Level of Defence in depth: Prevention of failures and abnormal operation**
- The primary way of preventing accidents is to achieve a high quality in design, construction and operation of the plant, and thereby to ensure that deviations from normal operation are infrequent

IAEA

Defence in depth (cont.)

Independence of levels of defence in depth

NSR-2/1 Rev 1. 4.13a: "*The levels of defence in depth shall be independent 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*".

Factors that affect the independence of levels of defence in depth

- Sharing of systems or parts of them to perform functions belonging to different levels of defence (e.g. common power supply, common cooling systems)
- Exposure to common cause failures (e.g. internal or external hazards)

IAEA

Radiation protection

SSR-2/1 Req. 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 the dose limits, that they are kept as low as reasonably achievable in operational states for the entire lifetime of the plant, and that they remain below acceptable limits and as low as reasonably achievable in, and following, accident conditions.

Radiation protection of the public and environment

Normal Operation

- The releases and the doses should comply with the prescribed limits and should be ALARA.

Accident conditions

- The releases and the doses evaluated in the accident analysis* should comply with the acceptable limits for each category of accidents as established by the Regulatory Body.

IAEA

(*) Normally included in a dedicated chapter of the SAR

Radiation protection (cont.)

Radiation protection of the workers at the plant *

- All actual and potential sources have to be identified
- The materials have to be selected to minimize the activation, the generation and transport of corrosion products and activation products shall be controlled
- Provisions shall be made for preventing the release or dispersion of radioactive substances
- The plant layout shall ensure that areas with radiation hazards and possible contamination are adequately controlled
- The plant shall be divided in zones related to the expected occupancy and radiation levels
- Shielding shall be provided to prevent or reduce radiation level
- Equipment subject to frequent maintenance or manual operations shall be located in areas of low dose rate
- Facilities shall be provided for the decontamination of personnel and equipment
- Equipment shall be provided for radiation monitoring in operational states and accident conditions

(*) Normally included in a dedicated chapter of the SAR

Safety Classification of SSCs

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 frequency with which the item will be called upon to perform its function
  - the time following a PIE at which, or the period for which, the item will be called upon to perform a safety function.
- The safety classification affects the design rules, the quality requirements, the manufacturing process, the maintenance requirements and the cost

IAEA

Protection against internal and external hazards

SSR-2/1 Req. 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 for determination of the postulated initiating events and generated loadings for use in the design of relevant items important to safety for the plant

Internal hazards

Fire

Explosions

Flooding

Missile generation

Collapse of structures and falling objects

Pipe whip

Jet impact

External hazards

Natural

Meteorological events

Hydrological events

Geological events

Seismic events

Human induced

Aircraft crashes

Fire, explosions, missiles, release of toxic gases

IAEA

Protection against internal and external hazards (cont.)

- Items important to safety shall be designed and located to withstand the effects of hazards
- Hazards (e.g. fire, flooding or earthquakes) could potentially impair several levels of defence (for example, they could cause failures and, at the same time, inhibit the means of coping with such situations).
- Effective protection against fire requires prevention, detection and the limitation of consequences by creating different fire zones and physical separation (e.g. the redundant trains of safety systems) and fire extinguishing systems.
- The design shall provide for an adequate margin against levels of external hazards derived from the site evaluation

IAEA

Reliability of structures systems and components

SSR-2/1 Req. 23: Reliability of items important to safety

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

- SSCs important to safety shall be designed, qualified, procured, commissioned, operated and maintained to withstand with sufficient reliability the conditions specified in their design basis
- Potential for “common cause” failures shall be considered to determine the application of redundancy, diversity and independence
- “Single failure criteria” shall be applied to each safety group (required for safety systems; not required for safety features for DECs)
- The principle of the “fail safe design” shall be considered and incorporated into the design of systems and components in order that fails lead to a safe state

IAEA

Calibration, testing, maintenance, repair inspection and monitoring

SSR-2/1 Req. 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.

- The design shall be such that these activities can be performed according to relevant codes and over the life time of the plant and without undue radiation exposure of the workers
- For calibration, testing and maintenance during power operation, the plant design shall be such that these activities are facilitated and performed with no significant reduction in the system reliability

IAEA

Equipment qualification

SSR-2/1 Req. 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.

- Examples of environmental conditions are: vibration, temperature, pressure, jet impingement, electromagnetic interference, irradiation, humidity

IAEA

Ageing and wear- out

SR-2/1 Req. 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.

- Margins shall be provided to take into account ageing and wear-out mechanisms
- Provision shall be made for monitoring, testing, sampling and inspection to assess ageing mechanisms predicted at the design stage and to identify unanticipated degradation that may occur in service

IAEA

Human factors

SSR-2/1 Req. 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.

- The need for intervention by the operator on a short time shall be kept to a minimum, and it shall be demonstrated that the operator has sufficient time to make a decision and sufficient time to act.
- Design shall facilitate the optimal performance of the operator
- The design shall be “operator friendly” to avoid human errors and limit the effects of human errors
- The working environment shall be designed according to ergonomic principles
- The human-machine interface shall be designed to provide the operators with comprehensive but easily manageable information, compatible with the necessary decision and action time

...Thank you for your attention

IAEA