INPRO Dialog Forum-7: Sustainability of NES Based on Evolutionary Reactors

19-22 November 2013, Vienna

Safety Assessment and NPP Design Requirements

Hussam Khartabil

Division of Nuclear Installation Safety
Outline

- Introduction
  - Relation to INPRO methodology
    - IAEA safety fundamentals
    - Relevant Safety Standards
- IAEA Requirements for Safety Assessment
- IAEA Safety Requirements for the Design of NPPs
- Generic Reactor Safety Review
Introduction

A Few Observations (INPRO Safety Manual)

• In the area of safety, the basis for the development of INPRO BPs, URs and Criteria are the following IAEA Safety Standards
  • Fundamental Safety Principles
  • Requirements for the Safety Assessment for Facilities and Activities
  • Requirements for the Safety of Nuclear Power Plants
• These Safety Standards are applicable to existing, new and innovative designs of nuclear power plants
  • Applicable to “Reference Design” and new design being assessed (reference and new design are both expected to comply)
• The purpose of the INPRO assessment is to confirm “long term sustainability”
  • In the area of safety, asks for improvements over a Reference Design
  • It is not part of a licensing process; does not evaluate compliance with IAEA safety standards
• Results of safety assessment (e.g., safety analysis report) for both reference and assessed designs are pre-requisites (input) for performing INPRO assessment
  • The INPRO assessor is expected to be familiar with applicable requirements (e.g., IAEA Safety Standards)

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

Protective Actions to Reduce Existing Or Unregulated Radiation Risks

Emergency Preparedness and Response

Prevention of Accidents

Protection of Present and Future Generations

Justification of Facilities and Activities
Optimization of Protection
Limitation of Risks to Individuals

Role of Government
Leadership and Management for Safety

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

10 Safety Principles

Six Safety Principles selected by INPRO to develop “Basic Principles” in the area of safety

IAEA Safety Standards
for protecting people and the environment

Fundamental Safety Principles
IAEA Safety Standards
No. SF-1

IAEA Safety Fundamentals
for protecting people and the environment

Safety Fundamentals
Safety Requirements
Safety Guides

IAEA

Safety objectives and safety principles
Functional conditions required for safety
Guidance on how to fulfill the requirements


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

Protective Actions to Reduce Existing Or Unregulated Radiation Risks

Emergency Preparedness and Response

Prevention of Accidents

Protection of Present and Future Generations

Justification of Facilities and Activities
Optimization of Protection
Limitation of Risks to Individuals

Role of Government
Leadership and Management for Safety

Six Safety Principles selected by INPRO to develop “Basic Principles” in the area of safety
Requirements for Safety Assessment

- Applicable to all facilities and activities
- Facilities include: NPPs, research reactors, critical assemblies, fuel cycle facilities, irradiation facilities, etc.
- Activities include: Production, use, import and export of radiation sources, transport of radioactive material, decommissioning and dismantling of facilities, etc.
IAEA Safety Assessment Process

R1: Graded approach
R2: Scope of the safety assessment
R3: Responsibility for the safety assessment
R4: Purpose of the safety assessment
R5: Preparation for the safety assessment
R6: Assessment of the possible radiation risks
R7: Assessment of safety functions
R8: Assessment of site characteristics
R9: Assessment of the provisions for radiation protection
R10: Assessment of engineering aspects
R11: Assessment of human factors
R12: Assessment of safety over the lifetime of a facility or activity
R13: Assessment of defence in depth
R14: Scope of the safety analysis
R15: Deterministic and probabilistic approaches
R16: Criteria for judging safety
R17: Uncertainty and sensitivity analysis
R18: Use of computer codes
R19: Use of operating experience data
R20: Documentation of the safety assessment
R21: Independent verification
R22: Management of the safety assessment
R23: Use of the safety assessment
R24: Maintenance of the safety assessment
IAEA Relevant Safety Guides for Safety Assessment

Safety Fundamentals
- Safety objectives and safety principles

Safety Requirements
- Functional conditions required for safety
- Guidance on how to fulfill the requirements

IAEA Safety Standards
- Safety Assessment for Facilities and Activities
  - General Safety Requirements Part 4
    - No. GSR Part 4

IAEA Safety Standards Series
- Deterministic Safety Analysis for Nuclear Power Plants
  - Specific Safety Guide No. SSG-2
- Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants
  - Specific Safety Guide No. SSG-3
- Development and Application of Level 2 Probabilistic Safety Assessment for Nuclear Power Plants
  - Specific Safety Guide No. SSG-4
- Format and Content of the Safety Analysis Report for Nuclear Power Plants
  - SAFETY GUIDE No. GS-0-4.4

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.
# Contents of the Requirements for the Design

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

82 REQUIREMENTS

(“SHALL” STATEMENTS)
Generic Reactor Safety Review (GRSR)

- Based on IAEA requirements for
  - Safety assessment for facilities and activities (GSR Part)
  - Safety of nuclear power plant design (SSR-2/1)
- Can be carried out at any design stage of a new reactor: conceptual design to a design supported by a comprehensive preliminary safety analysis report (graded approach)
**Possible Grouping of Requirements from GSR-4 and SSR-2/1**

- Start with GSR-4 (generic requirements for facilities and activities) and supplement with NNP Design Requirements

<table>
<thead>
<tr>
<th>Requirement</th>
<th>GSR Part 4</th>
<th>Relevant paragraphs from SSR-2/1</th>
<th>Supplementary SSR-2/1 Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>1: Graded approach</td>
<td>3.1 – 3.7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2: Scope of the safety assessment</td>
<td>4.1 – 4.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3: Responsibility for the safety assessment</td>
<td>4.3 – 4.17</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4: Purpose of the safety assessment</td>
<td>4.18</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5: Preparation for the safety assessment</td>
<td>4.19</td>
<td>4.1, 4.2, 5.23</td>
<td>23, 29</td>
</tr>
<tr>
<td>6: Assessment of the possible radiation risks</td>
<td>4.20-4.21</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7: Assessment of safety functions</td>
<td></td>
<td>4.7, 5.75, 5.76</td>
<td>19, 20</td>
</tr>
<tr>
<td>15: Deterministic and probabilistic approaches</td>
<td>4.53-4.56</td>
<td>4.7, 4.17, 5.75, 5.76</td>
<td></td>
</tr>
<tr>
<td>Remaining Requirements from SSR-2/1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14: Design basis for each item important to safety</td>
<td></td>
<td>5.3</td>
<td></td>
</tr>
<tr>
<td>15: Design limits be specified</td>
<td>5.4</td>
<td>5.26</td>
<td></td>
</tr>
<tr>
<td>20: Design extension conditions</td>
<td></td>
<td>5.27-5.31</td>
<td></td>
</tr>
<tr>
<td>43 &amp; 44: Fuel elements and assemblies (one sheet)</td>
<td></td>
<td>6.1 - 6.3 + 44</td>
<td></td>
</tr>
<tr>
<td>45: Control of the reactor core</td>
<td>6.4 - 6.6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>46: Reactor shutdown</td>
<td>6.7 - 6.12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>82: Means of radiation monitoring</td>
<td>6.77-6.82, 6.83, 6.84</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
GRSR Process

- Statement of requirement(s) and related paragraphs
- Interpretation (IAEA guidance and other documents useful)
- Determine if information provided in a safety assessment is adequately addressing the requirements
- Review is done by a group of experts
  - Recognize good practices or shortcomings from previous review; recognize if additional material is needed, etc
Examples (1/7)

• GSR-4 Requirement 1: Graded Approach
  • A graded approach shall be used in determining the scope and level of detail of the safety assessment carried out in a particular State for any particular facility or activity, consistent with the magnitude of the possible radiation risks arising from the facility or activity

• Interpretation for NPPs
  • Availability of a safety analysis report consistent with the status of development of a new reactor
  • All GSR-4 and SSR-2/1 requirements should be evaluated. It should be noted which requirements are not yet addressed (taking status of development into consideration)
  • The reviewer needs to determine whether
    • The plant layout and systems are clearly described
    • A complete set of basic and derived acceptance criteria are provided
    • Where available, the preliminary analyses address the requirements
    • Areas of lacking maturity of development are identified
    • Areas of information to be completed are identified
Examples (2/7)

• Defence in Depth
  • GSR-4 Requirement 13: Assessment of defence in depth (generic requirement for all facilities and activities)
    • 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
  • SSR-2/1 Requirement 7: Application of defence in depth
    • The design of a nuclear power plant shall incorporate defence in depth. The levels of defence in depth shall be independent as far as is practicable
    • Followed by several paragraphs addressing issues such as availability of all levels of defence under continued operation, conservative design, use of inherent and engineered features, multiple means of ensuring fundamental safety functions, etc.
Plant States (changes in new design requirements)

<table>
<thead>
<tr>
<th>Operational states</th>
<th>Accident conditions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal operation</td>
<td>beyond design basis accidents</td>
</tr>
<tr>
<td>Anticipated</td>
<td>(a) design basis accidents</td>
</tr>
<tr>
<td>Operational</td>
<td>(b) severe accidents</td>
</tr>
<tr>
<td>Occurrences</td>
<td>accident management</td>
</tr>
</tbody>
</table>

(a) Accident conditions which are not explicitly considered design basis accidents but which are encompassed by them.
(b) Beyond design basis accidents without significant core degradation.
SSR-2/1 Requirement 19: Design Basis Accidents

A set of accident conditions that are to be considered in the design shall be derived from postulated initiating events for the purpose of establishing the boundary conditions for the plant to withstand without acceptable limits for radiation protection being exceeded.

- DBAs are used to define the design basis of the safety systems and for other items important to safety that are necessary to control those accidents (return the plant to a safe state and mitigate the consequences).

- Key plant parameters do not exceed specified design limits. No or only minor radiological impacts, both on and off the site, and do not necessitate any off-site intervention measures.

- Design Basis Accidents shall be analysed in a conservative manner.
SSR-2/1 Requirement 20: Design Extension Conditions

A set of design extension conditions shall be derived on the basis of engineering judgement, deterministic assessments and probabilistic assessments for the purpose of further improving the safety of the nuclear power plant by enhancing the plant’s capabilities to withstand, without unacceptable radiological consequences, accidents that are either more severe than design basis accidents or that involve additional failures. These design extension conditions shall be used to identify the additional accident scenarios to be addressed in the design and to plan practicable provisions for the prevention of such accidents or mitigation of their consequences if they do occur.

- The main purpose of DECs is to ensure that accident conditions not considered as DBAs are prevented and/or mitigated as far as reasonably practicable
- Used to define the design basis for the safety features and for the other items important to safety necessary to prevent and to mitigate DECs
- Design Extension Conditions can be analysed with a best estimate analysis
Examples (6/7)

Qualitative success criteria for Design Extension Conditions

- Significant releases are *practically eliminated* (*
- The integrity of the containment is maintained (the containment shall cope with core melt situation) and the plant can be brought into a controlled state
- For those conditions that are not practically eliminated design provisions shall be made such that only protective measures that are of limited scope in terms of area and time are necessary for the protection of the public, and sufficient time is available to implement these measures

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

• Paragraph 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

• The reviewer looks for demonstration of an appropriate programme of research, analysis and testing for innovative improvements
Summary

• INPRO assessor in the area of safety needs to be familiar with relevant IAEA Safety Standards
  • Safety Fundamentals (SF-1)
  • Requirements for safety assessment (GSR-4)
  • Requirements for NPP design (SSR-2/1)
  • Applicable safety guides
• GRSR Service methodology provides framework for design safety review for new reactors
• Review can be tailored to take reactor development stage into account
  • All requirements need to be addressed and eventually complied with as the design matures
THANK YOU
FOR
YOUR ATTENTION

h.khartabil@iaea.org