NUSSC WG Meeting on
DS508 – Safety Guide on Assessment of the Application of General Requirements for Design of Nuclear Power Plants

Javier Yllera
Safety Assessment Section
Division of Nuclear Installation Safety
DPP for DS508

- First proposal to NUSC in June 2017 including gaps originated by superseding NS-G 1.2, Safety Assessment and Verification.

- IAEA was requested to narrow the scope with DEC and Practical Elimination highlighted as focal topics of interest.

- New DPP prepared with involvement of interest countries focused on these topics, framed under the application of “Assessment of the Application of General Requirements for Design of Nuclear Power Plants” (preliminary title)

- DPP approved by CSS in April 2018

4. OBJECTIVE

The objective of this safety guide is to provide recommendations on the assessment of the implementation of selected requirements in SSR 2/1, Rev.1, and GSR Part 4, Rev. 1, relating to defence in depth and practical elimination of event sequences leading to early radioactive releases or large radioactive releases.

5. SCOPE

The scope of this safety guide will cover the assessment of the defence in depth implementation and the practical elimination of event sequences leading to early radioactive releases or large radioactive releases. Special attention will be given to the assessment of design extension conditions and the requirement for independence of safety systems from safety features for design extension conditions (especially features for mitigating the consequences of accidents involving the melting of fuel).

The most relevant requirements for this purpose in GSR Part 4 include the requirements:

- 7: Assessment of safety functions and
- 13: Assessment of defence in depth

Together with their corresponding requirements for NPP design in SSR 2/1, rev. 1:

- 4: Fundamental safety functions
- 7: Application of defence in depth

The application of these requirements is closely related to other requirements for general plant design in SSR 2/1, rev. 1, such as:

- 13: Categories of plant states
- 16: Postulated initiating events
- 19: Design basis accidents
- 20: Design extension conditions and
- 21: Physical separation and independence of safety systems

Which will be taken into account in the safety guide in as much as they are related to the implementation and assessment of defence in depth and safety functions, with specific focus on the aspects of design extension conditions and practical elimination event sequences that would lead an early radioactive release or a large radioactive release.
Developed with the following in mind: “What do I know about inspection now that I wish I knew as a new inspector?”

Proposed structure / table of contents

- Assessment of DiD
  - General part on DiD Implementation
- Assessment of different plant states
- Assessment of independence between different plant states

- Practical Elimination
  - Concept and interpretation
  - Identification of cases
  - Demonstration (general aspects)

- Annex. Demonstration of practical elimination for specific common cases

1. INTRODUCTION
2. OBJECTIVES AND SCOPE
3. STRUCTURE
4. ASSESSMENT OF DiD IMPLEMENTATION
   - DiD implementation strategy for new NPPs (general part)
     - Objective of levels of DiD and plant states
     - Assessment of effectiveness and reliability of the design provisions:
       - Identification of safety functions and challenging mechanisms (e.g., PIES, sequences, hazards and phenomenons)
       - Identification of safety provisions for the applicable plant state
     - Deterministic assessment (demonstration of compliance with applicable requirements supported by the complete safety analysis)
     - PSA (assessment of reliability of the design provisions)
     - Integration of deterministic and probabilistic assessment
   - Assessment of safety provisions for different plant states
     - Assessment of safety provisions for normal operation (all modes)
     - Assessment of safety provisions for abnormal operation
     - Assessment of provision for DBA
     - Assessment of provisions for DEC without significant fuel degradation
     - Assessment of provisions for DEC with core melt
   - Assessment of independence between safety provisions for different plant states
     - Functional independence between different plant states
     - Assessment of common cause failures and defensive mechanisms, including use of PSA for identification and assessment of dependencies
5. PRACTICAL ELIMINATION OF EVENT SEQUENCES THAT WOULD LEAD TO EARLY RADIOACTIVE RELEASES OR LARGE RADIOACTIVE RELEASES
   - Introduction, general aspects and interpretation of the concept for new NPPs
   - Identification of sequences to be practically eliminated
   - Demonstration of practical elimination (general aspects)
     - Physical impossibility
     - Very low likelihood with high confidence in the assessment
     - Elements of demonstration
6. REFERENCES,
7. ANNEX I: Assessment of practical elimination of specific common cases
   - Catastrophic break of major RCS equipment
   - Prompt reactivity accidents
   - Direct containment heating
   - Hydrogen explosions
   - Steam explosions
   - Severe accidents with containment by-pass, including open containment
   - Containment boundary melt through
   - Practical elimination of severe accidents at the spent fuel pool
   - (Other cases for non LWR reactors that could be identified)
Draft Development

- 1\textsuperscript{st} Consultancy Meeting April 2018
  - Countries / Organizations represented: Canada, France, Finland, Germany, UK, ENISS

- 2\textsuperscript{nd} Consultancy Meeting December 2018
  - Countries / Organizations represented: Canada, Czech. Rep., France, Germany, UK, ENISS

- 3\textsuperscript{rd} Consultancy Meeting End July 2019
  - Countries / Organizations represented: Canada, France, Japan, UK, ENISS

- Comments received on previous draft before and after the 3\textsuperscript{rd} meeting by USA, France, ENISS, Canada

- Comments received for this meeting from Canada, Egypt, Finland, Japan, Netherlands, Russian Federation, Sweden, Turkey, UK, USA, WNA and ENISS
### CONTENTS

1. **INTRODUCTION**............................................................................................................. 4  
   **BACKGROUND**........................................................................................................... 4  
   **OBJECTIVE**.................................................................................................................. 5  
   **SCOPE**.......................................................................................................................... 5  
   **STRUCTURE**................................................................................................................... 6

2. **THE OVERALL SAFETY APPROACH FOR DESIGN**..................................................... 7  
   **SAFETY AND RADIATION PROTECTION IN DESIGN**................................................. 7  
   **SAFETY ASSESSMENT: GENERAL OBJECTIVES**...................................................... 12  
   **MINIMIZATION OF THE RADIOLOGICAL CONSEQUENCES OF VERY UNLIKELY CONDITIONS EXCEEDING THE PLANT DESIGN ENVELOPE** 13

3. **IMPLEMENTATION AND ASSESSMENT OF THE CONCEPT OF DEFENCE IN DEPTH**.................................................................................................................. 19  
   **APPLICATION OF DEFENCE IN DEPTH TO THE DESIGN OF A NUCLEAR POWER PLANT**.................................................................................................................... 19  
   **ASSESSMENT OF THE IMPLEMENTATION OF THE DEFENCE IN DEPTH CONCEPT**............................................................................................................................... 26  
   **ASSESSMENT OF INDEPENDENCE BETWEEN SAFETY PROVISIONS FOR DIFFERENT PLANT STATES**......................................................................................... 31

4. **PRACTICAL ELIMINATION OF (PLANT CONDITIONS LEADING) EARLY RADIOACTIVE RELEASES OR LARGE RADIOACTIVE RELEASES**................................. 37  
   **IDENTIFICATION OF 'CREDDIBLE SEVERE ACCIDENT SEQUENCES' LEADING TO ACCIDENT CONDITIONS TO BE 'PRACTICALLY ELIMINATED'**........................................................................... 40  
   **IDENTIFICATION AND DESIGN OF PROVISIONS FOR PRACTICAL ELIMINATION**................................................................................................................................. 42  
   **DEMONSTRATION OF 'PRACTICAL ELIMINATION' (GENERAL ASPECTS)** .................... 44

**REFERENCES**...................................................................................................................... 49
Overview of the Draft Safety Guide
(condensed with respect to previous versions)

• The overall safety approach for design
  • Safety and radiation protection in design /Safety Assessment
  • Minimization of the radiological consequences of very unlikely conditions exceeding the plant design envelope

• Implementation and assessment of the concept of defence in depth
  • Application of defence in depth to the design of a nuclear power plant
  • Assessment of the implementation of the defence in depth concept
  • Assessment of independence between safety provisions for different plant states

• Practical elimination of early radioactive releases or large radioactive releases
  • Identification of ‘credible severe accident sequences’ leading to accident conditions to be ‘practically eliminated’
  • Identification and design of provisions for practical elimination
  • Demonstration of ‘practical elimination’. General aspects

Annex: Assessment of practical elimination of specific common cases
Why did we Departed from the DPP?

- SSG-2, rev. 1, meanwhile approved, addresses too many aspects in relation to PE or DEC, explaining the concepts, types of events or sequences to be considered for DEC and PE for the solely purpose of addressing the DSA aspects of them. Not clear what is DSA and role of DSA
- This poses very important constraints to what can be said in this safety guide as an approach to these topics.
- Naturally, SGs for design (Core cooling, containment, power supply, etc.) need to address specific design aspects related to DEC and PE as well.
- What is left for this safety guide? What can be said that it doesn’t overlap or contradict other guides (possibly not fully accurate)?
- This is why the original draft evolved to the safety approach providing a holistic perspective
Safety Analysis is only a part of Safety Assessment

- Safety **assessment** of NPPs verifies (in summary) that:

  1. Requirements for design (capability of SSCs, materials, safety class, codes and standards, EQ, protection against hazards, etc.), operation, etc. are met

  2. Then, in addition it needs to be demonstrated the plant, as designed, is capable of complying with acceptable limits on doses and discharges for different plant states (deterministic safety **analysis** (chapter 15)) within acceptable frequencies of occurrence (probabilistic safety **assessment**)

- DSA is not every aspect of safety assessment that is not PSA. The scope of SSG-2 is way too limited for that.
Overall Concept of Draft Safety Guide

- The guide addresses **concisely** the overall Safety Approach for Design, which provides a rationale for the family of the set of requirements in SSR 2/1, as a framework for addressing the topics of primary interest (DEC and Practical elimination). SSR 2/1 provides some top level description (no requirements) in chapter 2.


- An updated safety approach should consider the novelties of SSR 2/1, rev. 1:
  - Extension of the plant design envelope/basis to include design extension conditions
  - Need to demonstrate the practical elimination or event sequences leading to early or large releases
  - Minimization of the radiological consequences of very unlikely conditions exceeding the plant design envelope, e.g. extreme external hazards (This has caused a lot of confusion – clarification is needed)
Standards used as a basis

- GSR Part 4 does not address DEC or PE (These concepts are not applicable for activities and facilities at large)
- DID and safety functions are simplistic for activities and facilities (no reactivity control or residual heat removal in general, no need for 5 levels in general)
- Requirements in SSR 2/1 for
  - Radiation protection in design, Safety Functions, DiD and
  - DBA, DEC and safety assessment/analysis need to be the basis for the guide

With consideration of others as necessary
Foundations of NPP Safety - Safety Approach

Fundamental Safety Principles
Fundamental Safety Objective: Protect people and the environment
- No.5: Optimization of the protection
- No.6: Limitation of risks to individuals
- No.8: Prevention and mitigation of accidents

Fundamental Safety Functions
(for the irradiated fuel)
- Control of reactivity
- Removal of heat from the fuel
- Confinement of radioactive material and shielding

Defence in depth
Consecutive levels of protection (5), including physical barriers

Radiation Protection Req.5)
- Doses below limits and ALARA for each plant state category
- No need for off site protective actions in DBA
- “Large releases” practically eliminated

Requirements for Safety Provisions for different plants states for adequate levels or reliability
- PIEs, design limits
- safety classification, redundancy, physical separation, design for int/ext. hazards, qualification, fail-safe, etc.

(Not addressed)
# CONTENTS

1. INTRODUCTION .................................................. 1

2. SCOPE .......................................................... 1

3. SAFETY PRINCIPLES ........................................ 1

4. SAFETY APPROACH ........................................... 2
   4.1. Radiological protection and acceptance criteria .......... 3
   4.2. Design limits ............................................ 3
   4.3. Defence in depth ......................................... 3
   4.4. Postulated initiating events ............................. 5
      4.4.1. Internal events ................................... 5
      4.4.2. External events .................................. 6
      4.4.3. Combinations of events ......................... 6
      4.4.4. Common cause failure ........................... 7
   4.5. Safety functions ........................................ 7
   4.6. Reliability design ....................................... 7
      4.6.1. Redundancy ...................................... 7
      4.6.2. Diversity ......................................... 8
      4.6.3. Independence ..................................... 8
      4.6.4. Fail-safe design .................................. 9
      4.6.5. Auxiliary services ................................ 9
   4.7. Quality of plant ........................................ 10

5. DESIGN REQUIREMENTS ...................................... 11
   5.1. General design requirements ............................ 11
      5.1.1. Plant condition categories ...................... 11
      5.1.2. Design limits ................................... 13
      5.1.3. Performance requirements ....................... 13
      5.1.4. Codes and standards ............................ 14
   5.2. Design provisions against postulated initiating events .. 14
      5.2.1. Operational states ................................ 14
      5.2.2. Common cause failure .......................... 15
      5.2.3. Fires .............................................. 15
      5.2.4. Internal flooding ................................ 15
Requirement 14: Design basis for items important to safety

The design basis specifies for each structure, system and component (SSC) of the NPP:

- the functions to be performed, the operational states, accident conditions for which is needed
- the conditions generated by internal and external hazards that the SSC has to withstand
- the acceptance criteria for the necessary capability, reliability, availability and functionality
- specific assumptions and design rules

The design basis for each item important to safety shall be systematically justified and documented

<table>
<thead>
<tr>
<th>Operational states</th>
<th>Accident conditions</th>
<th>Design Extension Conditions</th>
</tr>
</thead>
<tbody>
<tr>
<td>NO</td>
<td>DBAs</td>
<td>Without significant fuel degradation</td>
</tr>
<tr>
<td>AOO</td>
<td></td>
<td>With core melting (severe accidents)</td>
</tr>
</tbody>
</table>

Loads and conditions generated by External & Internal Hazards (for each plant state)

Criteria for functionality, capability, margins, layout and reliability (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)

An extreme external hazard (beyond the design basis of important SSCs), e.g. external flooding, earthquake, may fail the most vulnerably safety equipment (small margins).

In this situation non-permanent equipment for power supply or cooling can prevent core damage or worse.

New requirements added in SSR 2/1, rev. 1 after the Fukushima accident to have provisions to connect non permanent equipment
<table>
<thead>
<tr>
<th>Level of defence Approach 1</th>
<th>Objective</th>
<th>Essential design means</th>
<th>Essential operational means</th>
<th>Level of defence Approach 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 1</td>
<td>Prevention of abnormal operation and failures</td>
<td>Conservative design and high quality in construction of normal operation systems, including monitoring and control systems</td>
<td>Operational rules and normal operating procedures</td>
<td>Level 1</td>
</tr>
<tr>
<td>Level 2</td>
<td>Control of abnormal operation and detection of failures</td>
<td>Limitation and protection systems and other surveillance features</td>
<td>Abnormal operating procedures/emergency operating procedures</td>
<td>Level 2</td>
</tr>
<tr>
<td>3a</td>
<td>Control of design basis accidents</td>
<td>Engineered safety features (safety systems)</td>
<td>Emergency operating procedures</td>
<td>Level 3</td>
</tr>
<tr>
<td>Level 3</td>
<td>Control of design extension conditions to prevent core melting</td>
<td>Safety features for design extension conditions without core melting</td>
<td>Emergency operating procedures</td>
<td>4a</td>
</tr>
<tr>
<td>3b</td>
<td>Control of design extension conditions to mitigate the consequences of severe accidents</td>
<td>Safety features for design extension conditions with core melting. Technical Support Centre</td>
<td>Complementary emergency operating procedures/ severe accident management guidelines</td>
<td>4b</td>
</tr>
<tr>
<td>Level 4</td>
<td>Mitigation of radiological consequences of significant releases of radioactive materials</td>
<td>On-site and off-site emergency response facilities</td>
<td>On-site and off-site emergency plans</td>
<td>Level 5</td>
</tr>
</tbody>
</table>
DiD

- It is not implemented equally for the reactor core, for the spent fuel pool or other radioactive sources (e.g. Effluents or gas systems)
- Countries in favour and against of dealing with DiD for more than reactor core, but a severe accident in the SFP is a case for practical elimination.
- Agreed to refer to different plant states instead of DiD levels already in the DPP (not unique association of DiD to plant states in relation to DEC-A). Some aspects of DiD level 1 re not only for normal operation (siting, safety culture, ISI, quality, etc.)
- Full independence in between DiD levels / Plant states is impossible. **Key aspect** for affordability: Safety provisions credited in an accident sequence for one plant state, e.g. AOO, cannot be credited for the next one, DBA.
Operational States | Accident Conditions
--- | ---
NO | DBAs (safety systems)
AOO | DECs

Acceptance Criteria

Acceptance Criteria
No need for off site protective actions

Acceptance Criteria
< large / early release

Operational Criteria

Acceptance Criteria

Residual risk

Plant Design Basis

Beyond Plant Design Basis

L1 | L2 | L3a | L3b | L4a | L4b | L5

Large Component Failure
Fast Reactivity Excursion

Operational Criteria

Acceptance Criteria

No need for off site protective actions

Acceptance Criteria

< large / early release

HPME
MCCI
H₂ Detonation
Containment Bypass

PRACTICALLY ELIMINATED
Frequency Example values

- NO limit for NO
- AOO limit

Consequences

- Acceptance criteria for DBA
- No need for offsite protective actions

Acceptance Criteria for DEC-B

Early/Large releases

Releases limited in area and time

Conditions Practically Eliminated

Design envelope basis

CDF goal per sequence

1.E-02 /y

LERF goal per sequence

Residual Risk region

Margin

No cliff edge

Below practical elimination

Below practical elimination
Frequency  

Example values  

NO  

AOO  
s  

DBA  

- DEC  

Acceptance criteria for DBA  
No consequences on population  

Acceptance criteria for DEC-B  

CDF goal per sequence  

LERF goal per sequence  

Consequences  

Margin  

No cliff edge  

Below practical elimination  

Residual Risk region  

AOO, normal case  

AOOS with failure of systems  

common for DBA: SBO, ATWS, etc.  

DBA, normal case  

Most Frequent DBAs  

Residual Risk region
Clarifications in relation to some comments
What is in DiD?

- All safety provisions are part of DiD (siting, design, operation and EPR), including those that contribute to the demonstration of Practical Elimination.
- There are conditions beyond the design basis for which accident management measures and emergency response measures are foreseen as part of the DiD.
- There are no measures beyond the DiD (they are not planned).
Clarifications in relation to some comments
Guide written for design or for safety assessment?
Important Topic to decide

• Since safety assessment verifies that the requirements for design are met, the guide can be written as for design, e.g. “safety provisions for DEC should be independent to the extent possible from…” or for assessment: “The safety assessment should demonstrate that safety provisions for …”

• However, it is not simple. Demonstrating the adequate implementation of DiD is much more complex than providing recommendations for its implementation. One approach provided in SR-46
Thank you!