Safety Principles and Defence-in-Depth Concept implemented in German Regulations

Kay Nünighoff, Shanna Eismar, Björn Becker, GRS

8 June 2017

International Conference on Topical Issues in Nuclear Installation Safety: Safety Demonstration of Advanced Water Cooled Nuclear Power Plants
German Safety Requirements

Revision of the German Regulations

- Former safety requirements partially date from the 1970s and 1980s
- New Safety Requirements for NPP developed between 2003 and 2012
  - last update in March 2015
  - specifies technical details to substantiate high level requirements in the Atomic Energy Act
  - take into account
    - the international state of the art in science and technology in the area of reactor safety and radiation protection and
    - existing German regulation and RSK guidelines
Defence-in-depth concept in German Safety Requirements for NPPs

- Allocation of **safety requirements** to all four levels of the defence-in-depth concept, especially
  - consistent **integration** of the **beyond-design-basis area** (Level 4) in the safety concept with the aim to control
    - events with (postulated) multiple failure of safety equipment,
    - phenomena resulting from accidents involving severe fuel damage (reactor core, spent fuel pool).

- The levels of defence are characterised by events and plant states of power operation and low-power and shutdown states as well as by equipment for their control.

- Fundamentally independent effectiveness of the equipment on the different levels of defence.

DiD-concept can be fully applied to the existing plants.
Technical Safety Concepts

- **Fundamental Safety Functions**
  - SiAnf 2.1
- **Barrier Concept**
  - SiAnf 2.2
- **Defence in Depth Concept**
  - SiAnf 2.3
- **Protection Concept against hazards**
  - SiAnf 2.4
- **Radiological Safety Objectives**
  - SiAnf 2.5
Radiological Safety Objectives

Level 1 and 2 (NO and AOO)
- Obeying dose limits according to radiation protection ordinance
- Dose minimization (ALARA) according to §6 of the radiation protection ordinance
- Monitoring of releases via defined release paths

Level 3 (DBA)
- No exceedance of emergency planning levels according to §49 of the radiation protection ordinance
- In addition, dose minimization according to §6 radiation protection ordinance have to be obeyed
- Analysis of all possible releases paths

Level 4a, 4b, and 4c (DEC)
- Minimizing of on-site and off-site radiological consequences
- Exclusion of
  - Early releases (early failure of bypass of containment)
  - Large releases (requiring wide area and long term counter measures off-site)
## Defence-in-depth Concept in Germany

<table>
<thead>
<tr>
<th>Level</th>
<th>Plant State</th>
<th>Measures</th>
<th>Safety objectives</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td><strong>Technical</strong></td>
<td><strong>Radiological</strong></td>
</tr>
<tr>
<td>1</td>
<td>Normal operation</td>
<td>Conservative design and high quality of technical equipment and operational measures</td>
<td>Avoid abnormal operation</td>
</tr>
</tbody>
</table>
| 2     | Anticipated operational occurrences | Control and limiting systems | • Control abnormal operation  
• Avoid occurrence of accidents | |
| 3     | Accidents (design basis accidents) | • Highly reliable safety systems  
• Reactor protection system | • Control accidents,  
• Prevent events involving the multiple failure of safety equipment, | Compliance with accident planning levels for the radiation exposure of the population and dose minimization requirement |
| 4a    | Very rare events | • Additional safety features and measures  
• Use of safety equipment | Control of events with postulated failure of the reactor scram system (ATWS) | Limitation of radiological consequences (minimisation requirement) |
| 4b    | Events involving the multiple failure of safety equipment | • Preventive measures of the internal accident management  
• Use of suitable respective measures and equipment of level of defence 1 to 3 | Control of events with multiple failure of safety systems to avoid accidents with severe core damage | |
| 4c    | Accidents involving severe fuel assembly damages | Mitigative measures of the internal accident management | Mitigate severe fuel assembly damages | |

### Prevention

- **Level 1**: Normal operation
- **Level 2**: Anticipated operational occurrences
- **Level 3**: Accidents (design basis accidents)

### Mitigation

- **Level 4a**: Very rare events
- **Level 4b**: Events involving the multiple failure of safety equipment
- **Level 4c**: Accidents involving severe fuel assembly damages

---

IAEA International Conference on Topical Issues in Nuclear Installation Safety 8 June 2017
Comparision with IAEA SSR-2/1

Comparison with international approaches

DiD in SSR2/1 → for new NPP
- Design: level 1 to level 4
- Level 1-3 → to prevent severe accidents
- Level 4 and 5 → to mitigate consequences of severe accidents

German DiD concept
- Same background → INSAG-10
- Level 1 to 3 comparable
- Level 4 is divided into 4a to 4c
- Level 4a and 4b still preventive
- Level 4c is mitigative
- “Level 5” is external plant accident management and civil protection
Comparison with WENRA-RHWG Safety Reference Level

**WENRA-RHWG** formulated **Design Extension Conditions** (DEC) for existing reactors (Issue F of the Safety Reference Levels) for existing reactors

- Since 2014: **two categories** for DEC
  - **DEC-A** for which **prevention** of severe fuel damage in the core or in the spent fuel storage can be achieved
  - **DEC-B** with postulated severe fuel damage

> WENRA-RHWGs Interpretation of DiD is **comparable** with the German understanding

<table>
<thead>
<tr>
<th>Operational States</th>
<th>Plant State</th>
<th>Safety Level</th>
<th>Plant State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal operation (NO)</td>
<td>1</td>
<td>Normal operation</td>
<td></td>
</tr>
<tr>
<td>Anticipated Operational Occurrences (AOO)</td>
<td>2</td>
<td>Abnormal operation</td>
<td></td>
</tr>
<tr>
<td>Design Basis Accidents (DBA)</td>
<td>3</td>
<td>Accidents (design basis accidents)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Accident Conditions</th>
<th>Safety Reference Level Issue F (Beyond design)</th>
<th>Plant State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Without significant fuel degradation (DEC-A)</td>
<td>4a</td>
<td>Very rare events</td>
</tr>
<tr>
<td>With core melt (DEC-B)</td>
<td>4b</td>
<td>Events involving the multiple failure of safety equipment</td>
</tr>
<tr>
<td></td>
<td>4c</td>
<td>Accidents involving severe fuel assembly damages</td>
</tr>
</tbody>
</table>
Comparison with WENRA Safety Objectives for New Reactors

DiD-concept for new reactors

- RHWG proposal
- Proposal and discussion also in IAEA-TECDOC-1791 (different approaches)

Differences:

- For new reactors core melt accidents are already considered in the design (Level 4)
- Postulated events are more comprehensive

No new NPP in Germany, but safety objectives for new NPP are considered in safety requirements (e.g. practical elimination)
Safety Objective: Practical Elimination

Radiological safety objective for new NPPs (WENRA-RHWG):

- accidents with core meltdown which would lead to early or large releases requiring measures of external accident management have to be practically eliminated;
- for accidents with core meltdown that have not been practically eliminated measures have to be taken so that only limited protective measures in area and time are needed for the public and that sufficient time is available to implement these measures.

- Also IAEA requirement for new NPP
- Aim to be achieved as reasonable practicable for existing NPP

- Fully adapted in German Requirements and implemented in the existing NPP
Implementation of Practical Elimination

Existing German NPPs: **Practical elimination demonstrated** by interaction of

- **plant operation** and
- high **reliability** of **safety systems** and
- comprehensive **plant internal accident management**

**Examples** for technical measures for the practical elimination of large and early releases:

- Primary system depressurisation
  - Prevention of high pressure core melt
- Filtered venting
  - Depressurization of the containment (e.g. non-condensable gases)
- Hydrogen management
  - Prevention of hydrogen detonation

Ensure integrity of the last barrier (containment)
Achieving Practical Elimination of Large and Early Releases

**Tier 1: Design of SSC of high reliability and quality**
- Concept of basic safety

**Tier 2: High reliable safety systems**
- Single failure concept

**Tier 3: Preventive accident management**
- Backfitting

**Tier 4: Mitigative accident management**
- SAMG

**Tier 5: Complementary PSA**
- Proof of low frequency
Vienna Declaration

**Principle 1:**

“New nuclear power plants are to be designed, sited, and constructed, consistent with the objective of preventing accidents in the commissioning and operation and, should an accident occur, mitigating possible releases of radionuclides causing long-term off-site contamination and avoiding early radioactive releases or radioactive releases large enough to require long-term protective measures and actions.”

No new NPPs in Germany, but **practical elimination of early and large releases** to be **demonstrated by interaction of**

- plant operation **and**
- high reliability of safety systems **and**
- comprehensive plant internal accident management

included in “Safety requirements for NPPs” published 2013
Principle 2:

“Comprehensive and systematic safety assessments are to be carried out periodically and regularly for existing installations throughout their lifetime in order to identify safety improvements that are oriented to meet the above objective. Reasonably practicable or achievable safety improvements are to be implemented in a timely manner.”

- Periodic Safety Review (PSR) required §19 Atomic Law
- NPPs in permanent shutdown before decommissioning perform similar safety reassessment according to rules for PSR
- 14 safety factors of IAEA SSG-25 implicitly covered in guidance documents published by BMUB
Vienna Declaration

** Principle 3:**

“National requirements and regulations for addressing this objective throughout the lifetime of nuclear power plants are to take into account the relevant IAEA Safety Standards and, as appropriate, other good practices as identified inter alia in the Review Meetings of the CNS.”

- Germany considers IAEA Safety Standards while developing or updating its regulatory framework.
- Germany has nuclear rules and regulations that have “grown” since the 1970s with the construction and operation of NPPs.
- Germany has a very specific implementation-oriented programme of nuclear standards (e.g. KTA).
- The IAEA Safety Standards are a fundamental basis for the definition of the state of the art in science and technology.
- Reference for updating the nuclear rules and regulations in Germany.
Conclusion

- International developments and recently published IAEA Requirements have been taken into account while drafting the German „Safety Requirements for NPPs“

- German DiD-concept meets international expectations for existing reactors
  - Objectives for new reactors serves as guidance for further improvement of nuclear safety

- Practical elimination of large and early releases
  - Implemented as an radiological objective in German regulation
  - Has not been considered in original design of the existing fleet of German NPPs, but is demonstrated by interaction of different other means

- Requirements of the Vienna Declaration are fully implemented
  - Germany reported in its 7. National Report to CNS and will present this during the 7. Review Meeting in March 2017