Regulatory Requirements and Monitoring and Assessment of the Implementation of Defence in Depth

Senior Regulator’s Meeting
25 September 2014

Petteri Tiippana
Content

• Defense in Depth in the light of recent experience
• Defense in Depth and Finnish safety regulations
• Experience with the implementation and oversight of Defense in Depth
• Conclusions
Recent Experience and Defense in Depth

- **Forsmark event 2006**
  - Offsite grid disturbance resulted in voltage surge on the onsite power supply systems resulting in common cause failure in safety systems
  - Issues of generic nature (robustness of DiD Levels, Dependencies, Fail-safe design)

- **Tepco Fukushima Daichi Accident 2011**
  - Insufficient design basis against flooding resulted in common cause failure in safety systems
  - Issues with Fail-safe design, weaknesses in DiD levels as well as dependencies between DiD levels
Requirements for Defense in Depth in the Finnish Regulations and Guides

- **Nuclear Energy Act**
  - Section 7 b on Safety principle of defense-in-depth; safety of a nuclear facility shall be ensured by means of successive levels of protection independent of each other

- **Government Decree on the Safety of Nuclear Power plants (2013)** provides requirements for
  - functional safety with five levels of defense
  - independence between the levels
  - structural safety with barriers
  - application of redundancy, separation and diversity principles to ensure fulfillment of safety functions

- **YVL B1 Safety design of a nuclear power plant (2013)**
  - Detailed requirements for the application of DiD in the design of a NPP e.g. for DiD levels, independence of the levels, and strength of individual levels
## DiD Levels, Event Categories and Frequencies

<table>
<thead>
<tr>
<th>Level</th>
<th>Event Description</th>
<th>Frequency Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 1</td>
<td>Normal operation (DBC 1)</td>
<td></td>
</tr>
<tr>
<td>Level 2</td>
<td>Anticipated operational occurrences (DBC 2)</td>
<td>$f &gt; 10^{-2}$/a</td>
</tr>
<tr>
<td>Level 3a</td>
<td>Postulated accidents Class 1 (DBC 3)</td>
<td>$10^{-2}$/a &gt; $f &gt; 10^{-3}$/a</td>
</tr>
<tr>
<td></td>
<td>Postulated accidents Class 2 (DBC 4)</td>
<td>$f &lt; 10^{-3}$/a</td>
</tr>
<tr>
<td>Level 3b</td>
<td>Design extension conditions (DEC)</td>
<td>DEC A – CCF combined with DBC2 / DBC3&lt;br&gt;DEC B – Probable failure combinations&lt;br&gt;DEC C – Rare external events</td>
</tr>
<tr>
<td>Level 4</td>
<td>Severe accidents (SA)</td>
<td>Safety goals&lt;br&gt;CDF $&lt; 10^{-5}$/a; LRF $&lt; 5 \times 10^{-7}$/a</td>
</tr>
<tr>
<td>Level 5</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Implementing and overseeing DiD

- Operating NPPs and current DiD requirements
  - In particular robustness against extreme external hazards
  - In general robustness of levels and independence between levels
  - Redundancy, Diversity, Separation/Isolation within or (/and) between levels

- Consistent implementation of DiD in different technical disciplines e.g. Digital I&C

- Clarification of applied concepts with e.g. quantitative goals
  - e.g. practical elimination, reasonably achievable/practicable

- Regulatory inspection and assessment approaches and their focus on DiD, use of different analysis tools, PSRs)
Conclusions

- Defense in Depth has been and continues to be the key concept for safety of nuclear power plants – But needs to be reinforced (e.g. against external events, loss of power systems, malfunction or loss of I&C, loss of heat sink, spent fuel pools)
- Needs to be regulated – Requirements for the implementation of Defense in Depth are set in the Finnish regulations and regulatory guides
- For harmonizing Defense in Depth approaches and in particular the implementation of DiD, practical guidance is be needed (e.g. extreme external hazards)
- Role of operators and regulators in ensuring DiD is also maintained and improved when necessary during the lifetime of the NPP – use of deterministic and probabilistic tools, PSRs