Fukushima
– A Failure of Institutional Defence in Depth

By
Mike Weightman

International Conference on Topical Issues in Nuclear Installation Safety: Defence in Depth
21-24 October 2013, Vienna
Contents

• Some generic principles for Defence in Depth
• Application to Fukushima
• Implications of Fukushima for DiD
• A Strong Nuclear Safety System – the three main DiD barriers
• Some Sub-barriers
• Assuring Strong Nuclear Safety Systems Worldwide
Defence in Depth – what do we mean?

Classically, it’s about military strategies to defeat a much stronger enemy:

- Having diversity means not putting all your forces in one block. But also about giving ground to weaken and engulf your enemy with your strongest forces.
Defence in Depth – what do we mean?

Change in Roman state defence strategy around 400AC:

Away from just very strong front line with intelligence about attacking forces in neighbouring states to multi-layered and diverse means of defeating attackers
Defence in Depth – what do we mean?

Used in castle design for centuries but also attention to siting:
Defence in Depth – what we mean:
Some Principles

• Multiple layered defensive barriers
• Independence of Barriers
• Sub- barriers built on principles of:
  – diversity
  – redundancy
  – segregation
  – no single point failure
• But balance of barriers reflecting finite resources
## Technical Defence In Depth - Generally Described in Five Levels

<table>
<thead>
<tr>
<th>Level of defence in depth</th>
<th>Plant Status</th>
<th>Objective</th>
<th>Essential Means</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 1</td>
<td>Normal Operation</td>
<td>Prevention of abnormal operation and failures by design</td>
<td>Conservative design, construction, maintenance and operation in accordance with appropriate safety margins, engineering practices and quality levels</td>
</tr>
<tr>
<td>Level 2</td>
<td>Operational Occurrences</td>
<td>Control of abnormal operation and detection of failures</td>
<td>Control, limiting and protection systems and other surveillance features</td>
</tr>
<tr>
<td>Level 3</td>
<td>Accidents</td>
<td>Control of accidents within the design basis</td>
<td>Engineered safety features and accident procedures</td>
</tr>
<tr>
<td>Level 4</td>
<td>Beyond Design Base Accidents e.g. core melt accident</td>
<td>Control of severe plant conditions in which the design basis may be exceeded, including the prevention of fault progression and mitigation of the consequences of severe accidents</td>
<td>Additional measures and procedures to prevent or mitigate fault progression and for on-site emergency management</td>
</tr>
<tr>
<td>Level 5</td>
<td>Significant off site release of radioactivity</td>
<td>Mitigation of radiological consequences of significant releases of radioactive materials</td>
<td>Emergency management and on-site and off-site emergency response</td>
</tr>
</tbody>
</table>
## Technical Defence In Depth - Generally Described in Five Levels

<table>
<thead>
<tr>
<th>Level of defence in depth</th>
<th>Plant Status</th>
<th>Objective</th>
<th>Essential Means</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 1</td>
<td>Normal Operation</td>
<td>Prevention of abnormal operation and failures by design</td>
<td>Conservative design, construction, maintenance and operation in accordance with appropriate safety margins, engineering practices and quality levels</td>
</tr>
<tr>
<td>Level 2</td>
<td>Operational Occurrences</td>
<td>Control of abnormal operation and detection of failures</td>
<td>Control, limiting and protection systems and other surveillance features</td>
</tr>
<tr>
<td>Level 3</td>
<td>Accidents</td>
<td>Control of accidents within the design basis</td>
<td>Engineered safety features and accident procedures</td>
</tr>
<tr>
<td>Level 4</td>
<td>Beyond Design Base Accidents e.g. core melt accident</td>
<td>Control of severe conditions in which the design basis may be exceeded, including the control of fault progression and the consequences of severe accidents</td>
<td>Additional measures and procedures to prevent or mitigate fault progression and for on-site emergency management</td>
</tr>
<tr>
<td>Level 5</td>
<td>Significant off site release of radioactivity</td>
<td>Mitigation of radiological consequences of significant releases of radioactive materials</td>
<td>Emergency management and on-site and off-site emergency response</td>
</tr>
</tbody>
</table>
Post Fukushima

Reconsideration of the DiD concept:

• NEA Steering Committee Policy Debate
• Is there a better balance between prevention and mitigation?
• This Conference
• INSAG thinking about whether to revisit its existing guidance
• Has it failed?
Fukushima – A lack of defence in depth of the Nuclear Safety Institutional System

- Inadequate design basis for external events
- Inadequate internal challenge within TEPCO
- Inadequate peer group challenge from Japanese nuclear industry or from international peers
- Inadequate challenge from Japanese regulator
- Inadequate outcome from peer review of the regulator
- Inadequate challenge from stakeholders
- Underlying cultural and institutional failings
Fundamental lesson of Fukushima is that Technical DiD can be subject to common mode failure through Nuclear Safety Institutional System Failure:

Inadequate Defence in Depth of the Nuclear Safety Institutional System
Conclusion of Analysis

- Technical defence in depth approach and principles are basically sound
- Not applied properly
- Nuclear Institutional System did not address failing – not robust
- Need to use the same DiD concept and principles to build, assess and review and challenge the Nuclear Institutional System to improve
- Backed up by a new overarching peer review of a nation’s nuclear institutional system undertaken by IAEA and WANO joint teams to review and challenge
Nuclear Safety Institutional System Defence in Depth: 3 main barriers

- Level A – Strong competent Industry
- Level B – Strong competent Regulator
- Level C – Strong competent Stakeholders

Principle:

independence between Levels and underpinned by a strong vibrant safety culture - welcoming challenge, passion to improve, openness and transparency, and accountability as a way of life
What do I mean by strong?

Inner strength not brute strength:
• Strong enough to listen and absorb others’ ideas
• Strong enough to not be afraid of challenge
• Strong enough to welcome new ideas and learn from others
• Strong enough to tell it as it is
• Strong enough to recognise when you got it wrong and show that you are learning from it
What do we mean by a Strong Regulator?

• Powerful
  – but not looking to express power, in a sense failed if have to enforce although never afraid to do so if circumstances appropriate
  – power is not just legal power but power of arguments, skills, strategy, inner strength, capabilities and values,
• Not afraid to be proportionate
• Highest standards of technical and regulator excellence
• Independence in law, practice and culture – but greater independence means need for greater accountability
• Openness and transparency at core
• Welcomes challenge and seeking ways to learn and improve
• Outcome focused
• Strong values to earn respect
### Components of the Nuclear Industry Barrier in a State or Region

<table>
<thead>
<tr>
<th>I.1</th>
<th>I.2</th>
<th>I.3</th>
<th>I.4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Licensee</td>
<td>State/Region Industry Peer Pressure</td>
<td>International Industry Peer Pressure/Review</td>
<td>International Institutional Review</td>
</tr>
<tr>
<td>SQEP Technical/Design/operational capability</td>
<td>Safety Directors Forum, INPO, etc.</td>
<td>WANO Missions and Requirements</td>
<td>IAEA OSART, Design Review, Siting, etc Missions</td>
</tr>
<tr>
<td>Independent Nuclear Safety Assessment</td>
<td>Nuclear Industry Association, Nuclear Energy Institute, ANS</td>
<td>Bilateral/Multilateral Organisations e.g. CANDU Owners Group</td>
<td></td>
</tr>
<tr>
<td>Nuclear Safety Committee</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Nuclear Leadership/Culture/Values**
## Components of a Strong Institution Regulatory Barrier

<table>
<thead>
<tr>
<th>R.1</th>
<th>R.2</th>
<th>R.3</th>
<th>R.4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regulatory Authority</td>
<td>Special Outside Technical Advice</td>
<td>International Peer Pressure</td>
<td>International Peer Reviews</td>
</tr>
<tr>
<td>World Class Technical/Regulatory Capability</td>
<td>E.g. Standing Panel of experts nominated by stakeholders – CNI Advisory Panel/ Groupe Permanent d’ Experts</td>
<td>NEA CNRA &amp; CSNI committees and working groups</td>
<td>IAEA IRRS missions</td>
</tr>
</tbody>
</table>
| Organisational Structure with internal standards, assurance, OEF, policy, strategy, etc. | Special Expert Topic Groups  
- Fukushima  
- Aircraft Crash | WENRA – reference levels, reviews, groups | ENSREG Reviews |
| Accountability to Governing Body – Board, Commission, etc. |  | IAEA Safety Standard meetings, etc. |  |

**Nuclear Leadership/Culture/Values**
# Components of the Strong Stakeholder Institutional Barrier

<table>
<thead>
<tr>
<th>S.1</th>
<th>S.2</th>
<th>S.3</th>
<th>S.4</th>
<th>S.5</th>
<th>S.6</th>
<th>S.7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workers</td>
<td>Public</td>
<td>Parliament</td>
<td>National &amp; Local Gov.</td>
<td>Neighbours</td>
<td>Media</td>
<td>NGOs</td>
</tr>
</tbody>
</table>

- Industry and Regulatory Routine Supply of Information
- Routine Reports on Activities and Decisions
- Special Reports on Matters of Interest
- Responsiveness to Requests for Information
- Routine and Special Meetings

**Openness & Transparency, Accountability, Assurance – Industry/Regulator Culture and Capability**
Assuring a Strong Nuclear Safety Institutional System

- The Model of Strong Nuclear System for a MS cuts across several organisational systems – industry, regulators, governments, etc.
- And topic areas – organisational design, government agency structures, leadership, cultures and values
- Not covered in total by Any Existing Review Service
- Several Review Services touch on Particular Aspects: e.g. OSART, ISCA, IRRS, INIRM, etc
- But none give a Complete Overview of the System – nearest Integrated Nuclear Infrastructure Review Mission used for new entrants mainly
- Also, need WANO input especially on Industrial corporate/site structures, leadership and cultures
Proposal – New Cross Cutting Review Service for Nuclear Safety System

• Based on the Defence in Depth model of the nuclear safety assurance system
• At high level
• Using components from existing services and others as needed
• Run jointly by the IAEA and WANO, also using expertise of NEA
• Targeting the organisational, cultural, competence, values, etc. aspects of the system, independence of the barriers and sub-barriers and use of the principles of DiD
A Way Forward?

- Agree in principle – WANO & IAEA
- Review and Refine the Model
- Produce Guidance
- Pilot the Review Service
- Review and Refine Model, Guidance, Review Service
- Look to use as part of the Convention Review Process
Summary

• Defence in Depth as a concept for establishing effective technical barriers is still valid
• However, it may need re-balancing & reinforcing
• Fukushima teaches us that this it is not sufficient – you need an effective Nuclear Safety Institutional System build on the same DiD concept and principles
• Major independent barriers in the system:
  – Strong Nuclear Industry Barrier
  – Strong Nuclear Regulator Barrier
  – Strong Nuclear Stakeholder Barrier
• Need a new IAEA/WANO led review service to ensure such systems are in place worldwide feeding into Convention Review Meetings
To Better Serve the People & Society