Design Guide for Modification for Beyond Design Basis Accidents

IAEA-J4-TM-46463 TM for Evaluation of Design Safety

Derek Mullin
Senior Technical Advisor – Regulatory Affairs

New Brunswick Power Nuclear
Canada
Background

• Level 2 PSA requirements established in Canada in 2005
• Quantitative safety goals for existing reactors not specified
• RD-337 for new reactors identifies qualitative and quantitative safety goals. Generally on order of magnitude less than for existing reactors
• IAEA guidance (e.g. SSG-3) identifies safety goals for existing reactors of $1E-04/yr$ (Severe Core Damage) and $1E-05/yr$ (Large Release Frequency)
• Canadian PSAs developed to address IAEA guidance
Introduction

• Fukushima lessons learned:
  – Re-examine plant defense-in-depth for beyond design basis events
  – Re-evaluate external hazard magnitudes using modern techniques and up-to-date information

• Need to deal better with hazard magnitudes not considered in original CANDU plant designs

• All Canadian utilities have standard rigorous design processes

• For Beyond Design Basis events, need to allow alternate strategies using best estimate methods

• Increase flexibility in approach to allow increased flexibility in accident response
Introduction

• Increased flexibility cannot compromise existing design basis
• Could have direct impact on risk estimates and achieving safety goals
• Desire for inter-utility consistency in approach to design modifications and safety evaluations
• CANDU Integration Industry Team
• Design guide developed to address design modifications for beyond design basis events
• Involves engineered systems and portable equipment
Overall Objective

• The overriding objective is to ensure that modifications undertaken to manage and/or mitigate Beyond Design Basis Accident conditions will:
  a) Ensure that NPP functionality is not compromised under design basis conditions, and
  b) Deliver the required functionality with high confidence under the anticipated BDBA conditions.

• Canadian utilities are adopting a balanced approach to managing the consequences of low frequency, high impact event sequences
Approach

• Avoid strict adherence to normal rigorous, conservative design practice when considering Beyond Design Basis Events

• Reasonable amendments or alternatives are acceptable provided:
  1. The modification does not adversely affect the design basis functionality of the NPP,
  2. The modification delivers the required functionality with high confidence under the anticipated accident conditions, and
  3. The proposed engineering approach to addressing the Beyond Design Basis Accident condition is consistent with
     a. The Power Reactor Operating Licence requirements,
     b. The appropriate engineering codes and standards, and
     c. The overall practice of engineering.

• Consider carefully before applying approach
# Design Categories

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
<th>Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Existing engineering Structures, Systems, Components which can be called upon to manage BDBAs.</td>
<td>This category includes all permanently installed station SSCs, where operation outside and/or beyond the design basis of the SSC may be required under BDBA conditions.</td>
</tr>
<tr>
<td>2</td>
<td>Equipment upgrades installed on existing engineered SSCs to manage BDBAs.</td>
<td>This category includes any modification (either in terms of additional equipment or upgraded equipment) in any permanently installed station SSC, which is required to maintain essential functionality under BDBA conditions.</td>
</tr>
<tr>
<td>3</td>
<td>New engineered SSCs added for the sole purpose of managing BDBAs.</td>
<td>This category includes all new SSCs which are permanently installed specifically to manage and/or mitigate BDBA conditions. All connection points and/or interactions with existing SSCs must comply with the requirements for that SSC.</td>
</tr>
<tr>
<td>4</td>
<td>Portable SSCs which can be attached to an existing SSC to manage BDBAs.</td>
<td>This category includes all portable (or any temporarily connected) equipment and/or tools required to manage and/or mitigate BDBA events.</td>
</tr>
</tbody>
</table>
Design Requirements

• Although design guide addresses requirements for all categories, focus of presentation is on Category 3 and 4 only

• Establish Review Level Conditions for beyond design basis events

<table>
<thead>
<tr>
<th>Category</th>
<th>Basis</th>
</tr>
</thead>
<tbody>
<tr>
<td>3, 4</td>
<td>Review Level Condition beyond the design basis are specified and consistent with that used in Probabilistic Safety Assessment</td>
</tr>
<tr>
<td></td>
<td>Certain equipment may have more stringent Review Level Condition applied depending on the application</td>
</tr>
</tbody>
</table>
### Engineering Calculations and Analysis

<table>
<thead>
<tr>
<th>Category</th>
<th>Assumptions &amp; Input Data</th>
<th>Basis</th>
</tr>
</thead>
</table>
| All      | Best Estimate            | The best estimate approach (BEA) should be used when:  
  - Estimating plant conditions under which the equipment is expected to function  
  - Determining the capability and availability of other station equipment, except for that rendered unavailable or impaired by the BDBA  
  - Specific areas where BEA may be used include assessments of seismic conditions, harsh environment conditions, and so forth.  
  Care must be applied to ensure that potential hazards are not underestimated. Analyses of interactions with other (i.e. already installed) SSCs under design basis conditions should be performed using the normal (conservative) approach. |
Operating Instructions

• Impacts Human Reliability Analysis in PSA

<table>
<thead>
<tr>
<th>Category</th>
<th>Type</th>
<th>Basis</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Abnormal Plant Operating Procedures, Emergency Operating Procedures, Severe Accident Management Guidelines</td>
<td>Because these are permanently engineered SSCs, the normal suite of operating instructions should be used to operate these SSCs.</td>
</tr>
</tbody>
</table>
| 4        | Emergency Operating Procedures, Emergency Standard Operating Sequences, Severe Accident Management Guidelines | • Must be field verified and validated for clarity and usability.  
• Not normally be utilized except under extreme conditions, any requirement for the operator to be in attendance is highly dependent on the nature of the Beyond Design Basis Accident and habitability.  
• Habitability should be considered |
Procurement, Installation and Commissioning

• Specific requirements are included in design guide
• Not discussed further as safety evaluations generally assume correct equipment is procured, installed and commissioning correctly
• Probabilistic Safety Assessment addresses such issues that might degraded redundancy through inclusion if residual Common Cause Failure (CCF) events
## Maintenance

<table>
<thead>
<tr>
<th>Category</th>
<th>Process</th>
<th>Basis</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Emergency procedure practice(s)</td>
<td>Normal maintenance process and practices apply since this category is a permanently installed, engineered system.</td>
</tr>
<tr>
<td>4</td>
<td>Emergency procedure practice(s)</td>
<td>Maintenance activities should be based on manufacturer’s recommendations, and other sources (e.g. design input, Probabilistic Safety Assessment if credited).</td>
</tr>
</tbody>
</table>
Testing, Routines and Call-ups

- Drills and exercises may be sufficient
- Probabilistic Safety Assessment may impose more stringent requirements

<table>
<thead>
<tr>
<th>Category</th>
<th>Process</th>
<th>Basis</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Normal practice(s) (with appropriate consideration for BDBA)</td>
<td>Because these are permanently engineered SSCs, follow normal processes and practices to demonstrate availability. Overall operational requirements must be clearly specified and accepted by the station (i.e. through an Available For Service process or equivalent).</td>
</tr>
<tr>
<td>4</td>
<td>Emergency procedure practice(s)</td>
<td>Follow manufacturer’s recommendations, and other sources (e.g. design input, Probabilistic Safety Assessment if credited). No specific availability requirements unless specified by Probabilistic Safety Assessment and the site Reliability Program.</td>
</tr>
</tbody>
</table>
Human Factors/ Human and Organizational Performance

• Deployment strategies for Category 4 equipment shall consider Human Factors and Human and Organizational Performance

• Design should facilitate ease of deployment for connection of portable equipment (e.g. colour coding hoses)

• Connection points should be accessible without need for additional, temporary equipment (e.g. ladders)

• Impacts Human Reliability Analysis in Probabilistic Safety Assessment
Crediting Category 3 and 4 Equipment in Safety Evaluations

• For design basis accidents, Category 1 and 2 applies. Operator actions are clear and equipment can be credited in safety evaluations

• For beyond design basis accidents, not so clear...

• Mitigating strategies are dependent on nature of accident, availability of systems and equipment

• For Category 3 equipment, if last line of defense and decision criteria to use is clear, then it can be credited in safety evaluations
Crediting Category 3 and 4 Equipment in Safety Evaluations

• Two methods of utilization for Category 4 equipment (eg. Portable generators and/or portable pumps):
  – Severe accident prevention
    • Deployment called from typical emergency operating procedures
    • Clear entry criteria based on plant condition
    • Can be credited in safety evaluations
  – Severe accident mitigation
    • SAMG approach following fundamental safety principles
    • More complex event. Use of preferred, alternate strategies
    • No guarantee that certain decisions will be made. Therefore, no clear entry criteria
    • No clearly defined rules how and when equipment can be credited in safety evaluations
Other Evaluations

- **External Hazard Evaluations**
- **High winds, earthquakes, flooding**
- **Further work needed to ensure industry consistency;**
  - Decision criteria to determine when detailed PSA is required based on hazard magnitude and frequency
  - Aggregation of external hazards
  - Application and interpretation of safety goals
  - Methodology for external hazard PSAs including well documented technical basis
  - Treatment of very large uncertainties
Summary

• Accepted in Canada that a graded level of rigour may be applied to modifications intended to mitigating Beyond Design Basis Accidents

• Design guides have been developed that reflect:
  – Review Level Conditions for Beyond Design Basis events
  – Consistent Canadian utility approach
  – A structured, systematic and risk-based approach to modifications

• Approach aligns well with industry Fukushima Principles

• Further need to define rules and conditions under which Category 4, or portable Emergency Mitigating Equipment, may be credited in safety evaluations

• Further work needed to ensure consistency dealing with external hazard evaluations
Design Guide for Modification for Beyond Design Basis Accidents

IAEA-J4-TM-46463 TM for Evaluation of Design Safety

Derek Mullin
Senior Technical Advisor – Regulatory Affairs

New Brunswick Power Nuclear
Canada