Licensing Modernization Project: A Systems Engineering Approach to RIPB Design Safety and Licensing

Ed Wallace
ANS RP3C CoP
October 30, 2020
Disclaimer

The materials in this presentation have been selected from published works in the public domain and personal notes, works and comments of the speaker based on his direct involvement in many projects contributing to the development and understanding of RIPB practices for advanced nuclear power design and licensing. Other sources or uses may exist as well and no attempt has been made to fully cite all sources. The comments and remarks are the sole opinion of the author of this presentation and do not necessarily represent the opinion of ANS, RP3C or the original source authors.
Introduction and Welcome

• Ed Wallace – President, GNBC Associates, Inc
  • 50+ years in the nuclear industry
    • Nuclear Navy
    • Utilities – GPU Nuclear, TVA, Exelon
    • Developers – PBMR, NuScale Power
    • Consulting Clients – WEC, KEPCO, TransAtomic, Southern

• Academic Background
  • BS – US Naval Academy
  • Naval Nuclear Power School and Prototype Training
  • Graduate Studies - Stevens Institute
  • MBA – University of Tennessee – Chattanooga

• ANS Member – 2004 - present
  • ANS 53.1 WG – 2004-2010
  • Standards Board 2013- 2019
  • RP3C 2013-present (Vice Chair – 2013-2019)
NEVER CONFUSE SAFETY AND LICENSING!

LMP is about RIPB safety design    TICAP is about licensing
LMP Overview

• Purpose: provide an overview of LMP outcomes, content, context and some potential applications

• Major Outcomes
  • NEI 18-04 r1 “Risk-Informed Performance-Based Technology Inclusive Guidance for Non-Light Water Reactor Licensing Basis Development
  • Southern Company supporting reports on:
    • PRA Approach
    • LBE Selection
    • SSC Classification and Special Treatment
    • Defense-in-Depth Adequacy Evaluation
    • LMP Lessons Learned, Best Practices, and Frequently Asked Questions
  • Endorsement in NRC RG 1.233 r0 “Guidance for a Technology-Inclusive, Risk-Informed, and Performance-Based Methodology to Inform the Licensing Basis and Content of Applications for Licenses, Certifications, and Approvals for Non-Light Water Reactors”
LMP Purpose

From NEI 18-04 (LMP Guideline):

• ...The scope of this document is focused on establishing guidance for advanced (i.e., non-LWR) designs so license applicants can develop inputs that can be used to comply with applicable regulatory requirements, ...

Based on regulatory application requirements and their implementation guidance, an applicant must answer the following questions:

• What are the plant initiating events, event sequences, and accidents that are associated with the design?
• How does the proposed design and its SSCs respond to initiating events and event sequences?
• What are the margins provided by the facility’s response, as it relates to prevention and mitigation of radiological releases within prescribed limits for the protection of public health and safety?
• Is the philosophy of DID adequately reflected in the design and operation of the facility?
Systems Engineering Design Approach

Top Requirements
- User
- Owner/operator
- Regulator
- Vendor
- Government

1. Generate Energy for Steam and/or Electricity
   - Develop SSC design features and programmatic requirements for energy generation

2. Protect Plant and Process
   - Add design features and/or programmatic requirements for investment protection and reliability

3. Protect Offsite Public and Plant Workers
   - Add design features and/or programmatic requirements to assure public and workers protection with adequate Defense in Depth

4. Provide Emergency Planning
   - Specify emergency planning needed as part of Defense in Depth

Conventional Power Design Practices

Nuclear Design Safety Practices

Ref: NGNP-LIC-GEN-RPT-G-00026 October 2009
Figure 3-1

It starts from a through understanding of the Performance-Based Outcomes
LMP As an Additional Consideration in Design

An important LMP objective is to build this into the design, not bolt it on.

Ref: NGNP-LIC-GEN-RPT-G-00026 October 2009
Figure 3-2
Systems Engineering Applications in Practice

SE practices create the structure to build RIPB safety into designs. LMP assumed this would occur.

Figure Courtesy of Ralph Hill
Notional Phasing of RIBP Evolution in Design (MHTGR Example)

**Figure 3-3. Evolution of Design, PRA, and LBE Development for the MHTGR**

### RIPB Systems Engineering Elements (Partial)

<table>
<thead>
<tr>
<th>DESIGN DEVELOPMENT STAGE</th>
<th>CONTRACT TECHNICAL REQUIREMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>R&amp;D</td>
<td></td>
</tr>
</tbody>
</table>

#### Pre-Conceptual Design
- **Plant Functional & Performance Rqmnts**
- **Plant Hazard Identification**
- **Plant Risk Evaluation**
- **Plant F-C Curve**
- **Plant Safety Functions**
- **Binning?**

#### Conceptual Design
- **SS Functional & Performance Rqmnts**
- **SS Hazard Identification**
- **SS Risk Evaluation**
- **SS Safety Strategy & Safety Functions**
- **SS Safety Functions Allocation**
- **SS Safety Classification**
- **↑**
- **↑**
- **←**

#### Detailed Design
- **Product Functional & Performance Rqmnts**
- **Product Hazard Identification**
- **Product Hazard Evaluation**
- **Product Target Reliability**
- **Product Safety Classification**
- **PRODUCT BASELINE**
- **Binning?**

#### Building it into a Design Control Process is a Developer Responsibility! (Standards can help too!)

Table Courtesy of Ralph Hill

---

**GNBC ASSOCIATES**

10/30/2020  Presentation to ANS RP3C Community of Practice
LMP Methodology Overview

- These are tasks that must be addressed for a complete RIPB design development.
- The include traditional deterministic actions, PRA, and integrated RIPB decisions
- The task order is up to the design control process owner
- The process is iterative within design phases and across design phases
Licensing Basis Events (LBEs)

- LBEs are defined by event sequence families from design specific PRA
- Purpose is to evaluate risk significance of individual LBEs and SSCs and to help define the RSFs; not a regulatory acceptance criterion
- Derived from the NGNP F-C Target and frequency bins for AOOs, DBEs, and BDBEs
  - Modified to ensure risk target does not increase with decreasing frequency
- F-C Target anchor points based on:
  - 10 CFR 20 annual dose limits used to define iso-risk contour in AOO region
  - Avoidance of offsite protective actions for lower frequency AOOs
  - 10 CFR 50.34 dose limit for lowest frequency DBEs
  - Consequences based on 30 day TEDE dose at EAB
  - EAB dose target for BDBEs ensures meeting QHO for prompt fatality
- LBEs compared to F-C target based on mean, and upper (95%tile) and lower (5%tile) bound estimates of LBE frequency and dose
- Separate cumulative risk targets used to ensure that 10 CFR 20 and QHO met for the total risk over all the LBEs
F-C Target w/ Risk-Significance Criteria

- The boundary lines and regions provide the risk-informed context for design safety evaluation
- Keeping LBE risk low should be an objective and natural consequence of using the LMP methodology early in the design process

NEI 18-04: Figure 5-4. Integrated Process for Incorporation and Evaluation of Defense-in-Depth
Example of LBEs in an F-C Context
SSC Classification and Special Treatment in LMP

- **Required Safety Functions (RSFs)**
- **SR SSC Design Criteria (SRDC)**
- **Safety Related (SR) SSCs**
- **SR SSC Performance Targets**
- **SR SSC Special Treatment Requirements**
- **Design Basis Accidents (DBAs)**
- **Design Basis External Hazard Levels (DBEHLs)**
- **Non-SR with ST (NSRST) SSCs**
- **NSRST SSC Performance Targets**
- **NSRST SSC Special Treatment Requirements**
- **Non-SR with No ST SSCs (NST)**

**Fundamental Safety Functions (FSFs)**

- **PRA Safety Functions (PSFs)**
- **Frequency-Consequence and Cumulative Risk Targets**
- **LBES from LMP (AOOs, DBEs, and BDBEs)**

**Other Risk Significant Safety Functions**

**Other Safety Functions for Adequate DID**

**Other Safety Functions Provided in the Design**

**Other Safety Functions**
SSC Classification and Risk Significance

• A prevention or mitigation function of the SSC is necessary to meet the design objective of keeping all LBEs within the F-C target.
  • The LBE is considered within the F-C target when a point defined by the upper 95%-tile uncertainty of the LBE frequency and dose estimates are within the F-C target.

• The SSC makes a significant contribution to one of the cumulative risk metrics used for evaluating the risk significance of LBEs.
  • A significant contribution to each cumulative risk metric limit is satisfied when total frequency of all LBEs with failure of the SSC exceeds 1% of the cumulative risk metric limit. The cumulative risk metrics and limits include:
    • The total frequency of exceeding of a site boundary dose of 100 mrem <1/plant-year (10 CFR 20)
    • The average individual risk of early fatality within 1 mile of the Exclusion Area Boundary (EAB) < 5×10⁻⁷/plant-year (QHO)
    • The average individual risk of latent cancer fatalities within 10 miles of the EAB shall not exceed 2×10⁻⁶/plant-year (QHO)
SSC Classification Universe

NEI 18-04 Figure 4-2. Definition of Risk-Significant and Safety-Significant SSCs
Derivation of Special Treatment Requirements

• SR SSCs
  • Required Functional Design Criteria (RFDC) derived from Required Safety Functions (RSFs); may be used with ARDCs in formulating principle design criteria
  • Component level Safety Related Design Criteria (SRDC) developed from RSFs

• SR and NSRST SSCs
  • SSC reliability and capability performance targets
  • Focus on prevention and mitigation functions identified in LBEs
  • Integrated decision-making process to derive additional specific special treatment requirements, if any
  • Reflects concepts from 10 CFR 50.69 and NEI-00-04 from existing reactors from a “forward fit” perspective
  • Reflects Commission’s expectations for risk-informed and performance- based regulation from SRM to SECY 98-0144

See NEI18-04 Section 4 and 5
Layers of defense are defined that provide for the prevention and mitigation of adverse events. The actual layers and number are dependent on the actual source and hazard posing the threat.

Protective measures are defined for each layer of defense. These are the design, operational and programmatic features needed to ensure the functionality of each layer. The specific protective measures are dependent on the actual source and hazards posing the threat.

NEI 18-04 Figure 5-1. U.S. Nuclear Regulatory Commission’s Defense-in-Depth Concept
LMP Defense-in-Depth Framework
LMP DID Adequacy Evaluation Objectives

- Establish alignment with accepted definitions of the DID philosophy and describe how multiple layers of defense are deployed to establish DID adequacy.
- Describe how the concept of protective strategies of DID are used to evaluate DID attributes incorporated into the plant capabilities that support each layer of defense.
- Identify the importance of defenses against common cause failures and need to minimize dependencies among the layers of defense.
- Identify any single features that are over relied on and take appropriate compensatory actions.
- Summarize the programmatic attributes of DID to provide adequate assurance that the DID plant capabilities in the design are realized when the plant is constructed and commissioned and are maintained during the plant design life cycle.
- Discuss the roles of programmatic DID attributes to compensate for uncertainties, human errors, and hardware failures.
- Provide a DID Baseline of information for evaluating changes to the design or operations that could impair DID adequacy conclusions.
# Plant Capability DID Attributes

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Evaluation Focus</th>
</tr>
</thead>
</table>
| **Initiating Event and Event Sequence Completeness** | PRA Documentation of Initiating Event Selection and Event Sequence Modeling  
Insights from reactor operating experience, system engineering evaluations, expert judgment |
| **Layers of Defense**                          | Multiple Layers of Defense  
Extent of Layer Functional Independence  
Functional Barriers  
Physical Barriers |
| **Functional Reliability**                    | Inherent Reactor Features that contribute to performing PRA Safety Functions  
Passive and Active SSCs performing PRA Safety Functions  
Redundant Functional Capabilities  
Diverse Functional Capabilities |
| **Prevention and Mitigation Balance**         | SSCs performing prevention functions  
SSCs performing mitigation functions  
No Single Layer / Feature Exclusively Relied Upon |

**NEI 18-04 Table 5-3. Plant Capability Defense-In-Depth Attributes**
# Programmatic DID Attributes

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Evaluation Focus</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Quality / Reliability</strong></td>
<td>Performance targets for SSC reliability and capability</td>
</tr>
<tr>
<td></td>
<td>Design, manufacturing, construction, O&amp;M features, or special treatment sufficient to meet performance targets</td>
</tr>
<tr>
<td><strong>Compensation for Uncertainties</strong></td>
<td>Compensation for human errors</td>
</tr>
<tr>
<td></td>
<td>Compensation for mechanical errors</td>
</tr>
<tr>
<td></td>
<td>Compensation for unknowns (performance variability)</td>
</tr>
<tr>
<td></td>
<td>Compensation for unknowns (knowledge uncertainty)</td>
</tr>
<tr>
<td><strong>Offsite Response</strong></td>
<td>Emergency response capability</td>
</tr>
</tbody>
</table>

NEI 18-04 Table 5-5. Programmatic DID Attributes
## Integrated DID Adequacy Decision Attributes

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Evaluation Focus</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use of Risk Triplet Beyond PRA</td>
<td>What can go wrong?</td>
</tr>
<tr>
<td></td>
<td>How likely is it?</td>
</tr>
<tr>
<td></td>
<td>What are the consequences?</td>
</tr>
<tr>
<td>Knowledge Level</td>
<td>Plant Simulation and Modeling of LBEs</td>
</tr>
<tr>
<td></td>
<td>State of Knowledge</td>
</tr>
<tr>
<td></td>
<td>Margin to Performance-Based Targets and Limits</td>
</tr>
<tr>
<td>Uncertainty Management</td>
<td>Magnitude and Sources of Uncertainties</td>
</tr>
<tr>
<td>Action Refinement</td>
<td>Implementation Practicality and Effectiveness</td>
</tr>
<tr>
<td></td>
<td>Cost/Risk/Benefit Considerations</td>
</tr>
</tbody>
</table>

*NEI 18-04 Table 5-8. Risk-Informed and Performance-Based Decision-Making Attributes*
Detailed Integrated DID Framework

NEI 18-04 Figure 5-2. Framework for Establishing DID Adequacy
A Note on Terminology Lessons Learned

• LMP took particular efforts to define new terms with new meanings such as:
  • Licensing Basis Events (LBE)
  • Safety Significant (SS)
  • Required Safety Function (RSF)
  • Safety Related Design Criteria (SRDC)
  • Design Basis External Hazards Levels (DBEHL)
  • Non-Safety Related with Special Treatment (NSRST)

• These are all defined specifically in the Glossary of NEI 18-04

• LMP also avoided certain terms that have been used historically and they are intentionally avoided in this RIPB methodology such as:
  • Single Failure Criteria
  • Important to Safety
  • Regulatory Treatment of Non-Safety Systems
  • “Credited”
  • 10CFR50.69 “RISC” Categories

• These terms carry a great deal of regulatory baggage that is, in part, what the LMP modifies, enabling the affirmative safety case to be the safety focus.

• Future standards activities focused on RI or PB incorporation should adopt these newer terms or build on them to assist with terminology convergence
Key References:

1. NEI 18-04 Revision 1 “Risk-Informed Performance-Based Technology Inclusive Guidance for Non-Light Water Reactor Licensing Basis Development, August 2019 (also as ADAMS ML19241A472)

2. NRC Regulatory Guide 1.233 Revision 0, Guidance for a Technology-Inclusive, Risk-Informed, and Performance-Based Methodology to Inform the Licensing Basis and Content of Applications for Licenses, Certifications, and Approvals for Non-Light Water Reactors, 06/2020, (also ML20091L698. This contains a long list of additional references as well)


Overview-LMP Lessons Learned, Best Practices, and Frequently Asked Questions (Ref 8)

Table of Contents
1.0 Purpose
2.0 Introduction
3.0 Lessons Learned (3)
   3.1 Initiating Events; Failure Modes and Effects Analysis:
   3.2 PRA Model Structure
   3.3 SSC Classification and Applicable Design Codes
4.0 Best Practices (5)
   4.1 Project Management
   4.2 Designer Organizational Culture
   4.3 NRC Staff Expectations:
   4.4 Iterative Nature of Design
   4.5 Conflicting SSC Classification Among Design Team Parties
5.0 Frequently Asked Questions (32)
   5.1 Background
   5.2 Process
   5.3 PRA FAQ and Responses (13)
   5.4 LBE FAQ and Responses (4)
   5.5 SSC Classification FAQ and Responses (9)
   5.6 DID FAQ and Responses (4)
   5.7 Project Management Common FAQ and Responses (2)
6.0 References
Thank You!

Any further questions?