Risk Informed and Performance Based Evaluation of Defense-in-depth

Edward G Wallace[a], Karl Fleming[b], and Amir Aflazi[c]
[a] GNBC Associates, Inc., Denver, CO, USA[*]
[b] **KNF Consulting Services LLC**, Spokane, WA, USA
[c] Southern Company Services, Birmingham, AL, USA

Abstract:

This paper, one of a series of papers, provides a structured approach to Defense-in-Depth (DID) adequacy evaluations as an integral part of a process to make greater systematic use of present day risk practices and performance-based outcome objectives. The purpose of this series of papers is to summarize risk-informed and performance-based methods developed within the industry-led Licensing Modernization Project. This series of papers have been provided to the NRC and is being developed to support the NRC in the development of regulatory guidance to license future advanced non-LWR nuclear power plants. The approach embraces existing U.S. and international definitions and philosophies of DID that set the foundation for the evaluation. The proposed evaluation framework builds on the DID framework developed in the U.S. Department of Energy Next Generation Nuclear Plant project.

The proposed DID framework [4] is technology-inclusive, risk-informed, and performance-based (TI-RIPB). The approach to establishing DID adequacy involves the incorporation of DID attributes into the plant capabilities and programmatic elements of DID. The integrated evaluation of DID adequacy includes both quantitative elements to incorporate Risk-Informed and Performance-Based (RIPB) considerations and qualitative elements that address uncertainties and limitations in the quantitative models and supporting data.

Keywords: PRA, Defense-in-Depth, DID Adequacy Evaluation

1. INTRODUCTION

Establishing DID adequacy involves the incorporation of DID attributes into the plant capabilities and programmatic elements that demonstrate DID adequacy. DID adequacy results from a series RIPB decisions in which the DID philosophy is incorporated into a structured evaluation of the design, development of the plant PRA, selection of licensing basis events, safety classification of SSCs, and specification of performance requirements for SSCs including the radionuclide physical and functional barriers that are part of multiple layers of defense of public health and safety. Demonstration of DID adequacy assures that there are multiple layers of defense for risk significant challenges to the design and that the plant capabilities and programs that support each layer are provided in a manner that minimizes dependencies among these layers and assures that different sources of uncertainties in the plant capabilities are adequately addressed.

Achievement of DID adequacy results from a series of RIPB decisions in which DID attributes are incorporated into the design, operations and maintenance, development of the plant Probabilistic Risk Assessment [2], selection of Licensing Basis Events (LBEs) [1], safety classification of Structures, Systems, and Components (SSCs) [3], and specification of performance requirements for SSCs [3]. The SSCs include the radionuclide physical and functional barriers, equipment that performs safety functions that protect these barriers, and operational and emergency planning elements that comprise multiple layers of defense. Demonstration of DID adequacy ensures that there are multiple layers of

[*] ed.wallace@gnbcassociates.com

defense for risk-significant challenges to the design and that the plant capabilities and programs that support each layer are provided in a manner that minimizes dependencies among these layers.

Risk-informed evaluation of DID considers the integrated performance of all plant SSCs and associated programs to manage daily operational activities, transients, and accidents, including the evaluation of strategies for accident prevention and mitigation. The RIPB LBE scenario framework used in this evaluation defines the challenges to the plant safety features included in the plant design basis and beyond, and the scope of all deterministic and probabilistic safety evaluations. By examining event sequences across the whole spectrum of LBEs, a systematic assessment of DID can be accomplished.

This structured form of sequence definition lends itself to clarifying what is meant by prevention and mitigation balance, and to identifying which SSCs are responsible for different prevention and mitigation functions. This framework is then used for formulating DID strategies that can be implemented as part of the plant capability and programmatic DID elements covering the design, manufacturing, construction, testing, and operational activities that support reasonable assurance of adequate protection determinations of public radiological safety. When implemented, the DID framework provides a more objective means to answer the question for a specific design: "When is enough, enough?"

2. DEFENSE-IN-DEPTH PHILOSOPHY

The DID framework proposed in this document embraces the definitions of the DID philosophy provided by international regulatory authorities including the NRC and the International Atomic Energy Agency (IAEA). The philosophy of defense-in-depth (DID), multiple independent but complimentary methods for protecting the public from potential harm from nuclear reactor operation, has been applied since the dawn of the industry. While the term has been defined primarily as a general philosophy by the U.S. Nuclear Regulatory Commission (NRC), a formal definition that permits an objective assessment of DID adequacy has not been realized.

According to the NRC glossary [7], defense-in-depth is:

> ...an approach to designing and operating nuclear facilities that prevents and mitigates accidents that release radiation or hazardous materials. The key is creating multiple independent and redundant layers of defense to compensate for potential human and mechanical failures so that no single layer, no matter how robust, is exclusively relied upon. Defense in depth includes the use of access controls, physical barriers, redundant and diverse key safety functions, and emergency response measures.

The history of defense in depth is complex and lengthy. In NUREG KM-009 [5] the NRC observes the importance of layers of defense as a cornerstone protective strategy. This is depicted in Figure 1. From this generalized case, the use of PRA exposes the layers systematically and enables further evaluation of the available layers of defense, independence of the layers, roles of barriers, inherent features, active and passive SSCs and the associated programmatic features that collectively contribute to achieving reasonable assurance of adequate protection. This framework is also consistent with the "levels of defense" concept advanced by the IAEA in Reference 0. To align with this process, some adaptation of the IAEA levels of defense concept is reflected in Figure 2. Together, alignment between the two philosophies can be seen.

Figure 1 – Layers of Defense

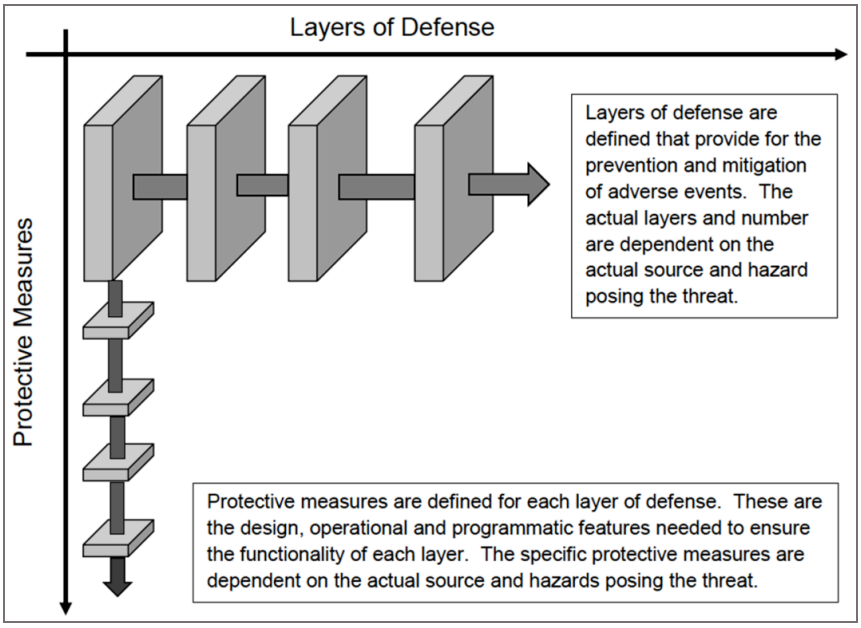
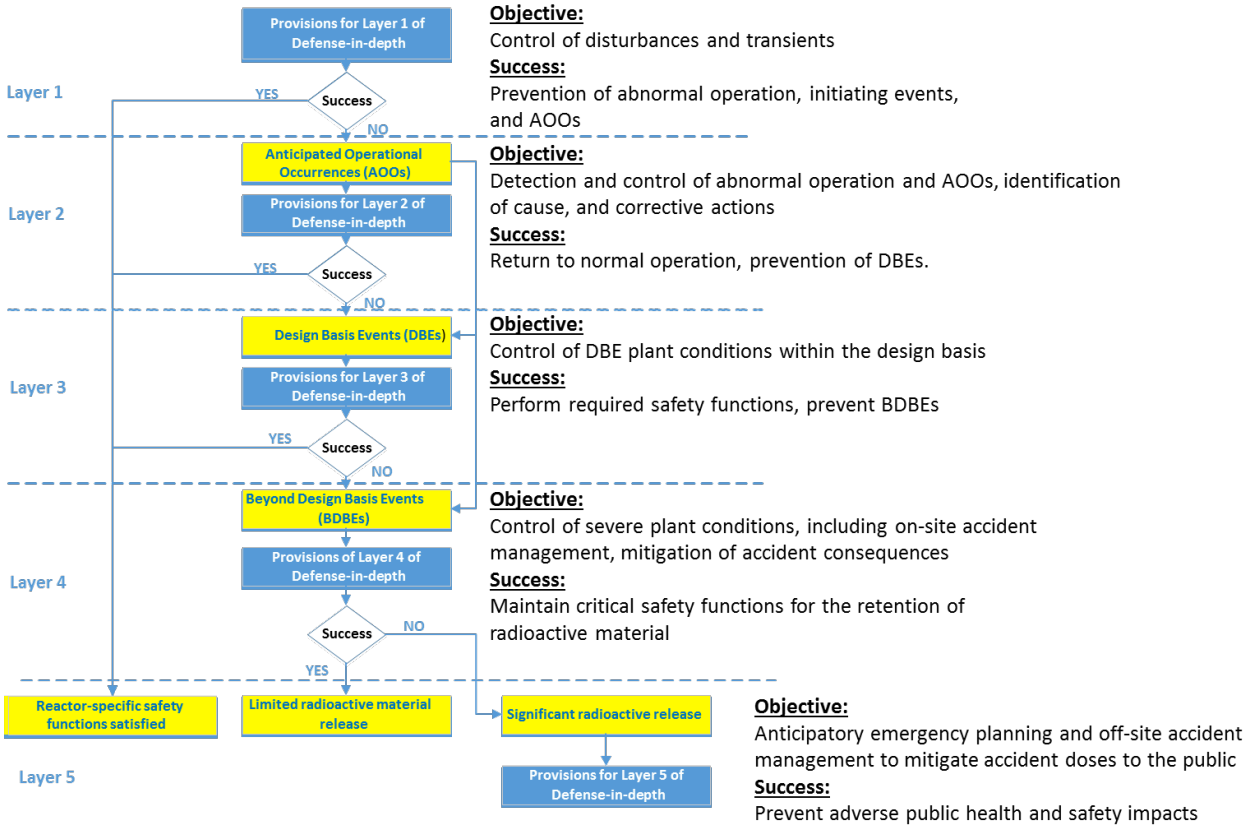


Figure 2 - Evaluating LBEs Using Layers of Defense Concept Adapted from IAEA[0]



The concept of protective strategies of DID are used to define DID attributes that are incorporated into the plant capabilities that support each layer of defense. The resolution of the general concept of protective strategies into a set of DID attributes is necessary to support an objective evaluation of DID adequacy.

3. DEFENSE-IN-DEPTH EVALUATION FRAMEWORK

When the framework is applied, sufficient information to make a structured and reproducible judgment about the adequacy of the DID provisions is developed. This information includes:

- A description of DID attributes appropriate for a TI-RIPB DID evaluation process
- Criteria and evaluation guidelines for determining DID adequacy, with the DID evaluation process including:
    - An evaluation of plant challenges, design features, operator responses, and administrative programs in an integrated manner as part of an overall risk management approach that utilizes both deterministic and probabilistic criteria
    - An evaluation of the uncertainties associated with the plant challenges and performance reflected in the risk evaluation and the identification of protective strategies to address them
    - An evaluation of the layers of defense reflected in the reliability, capability, and functional independence of plant capabilities
    - An evaluation of the balance among the plant capabilities and reliabilities for the prevention and mitigation of accidents
    - The selection of performance targets for the reliability and capability of the plant and SSCs, and provisions for monitoring of performance against these targets to provide confidence that guidelines for DID adequacy are achieved. The use of such targets and monitoring are essential to incorporate performance-based principles.
    - Quantitative elements to incorporate risk-informed and performance-based considerations and qualitative elements that address uncertainties and limitations in the quantitative models and supporting data and to incorporate risk insights

The general characteristics, from a process standpoint, required to be effective include:

.

- Systematic and Reproducible
- Sufficiently Complete
- Available for Timely Input to Design Decisions
- Risk-Informed and Performance-Based
- Reactor Technology-Inclusive
- Compatible with Applicable Regulatory Requirements

To effectively achieve these objectives, the evaluation of DID is broken down into a multi-part process as shown in Figure 3. In this figure, separate activities are undertaken to establish adequate Plant Capability DID and determine the appropriate Programmatic DID. These two activities become the foundation for an integrated RIPB evaluation of DID adequacy. The three major process elements are summarized below.

Plant Capability Defense-in-Depth

This element is used by the designer to select functions, structures, systems, and components and their bounding design capabilities to assure safety adequacy. Additionally, excess capability, reflected in the design margins of individual SSC and the use of redundancy and diversity, is important to the analysis of beyond design basis conditions that could arise. This reserve capacity to perform in severe events is consistent with the DID philosophy for conservative design capabilities that enable successful outcomes for unforeseen or unexpected events should they occur. Plant capability DID is divided into the following categories:

- Plant Functional Capability DID—This capability is introduced through systems and features designed to prevent occurrence of undesired LBE or mitigate the consequences of such events.

- Plant Physical Capability DID—This capability is introduced through SSC robustness and physical barriers to limit the consequences of a hazard.

These capabilities when combined create Layers of Defense response to plant challenges.

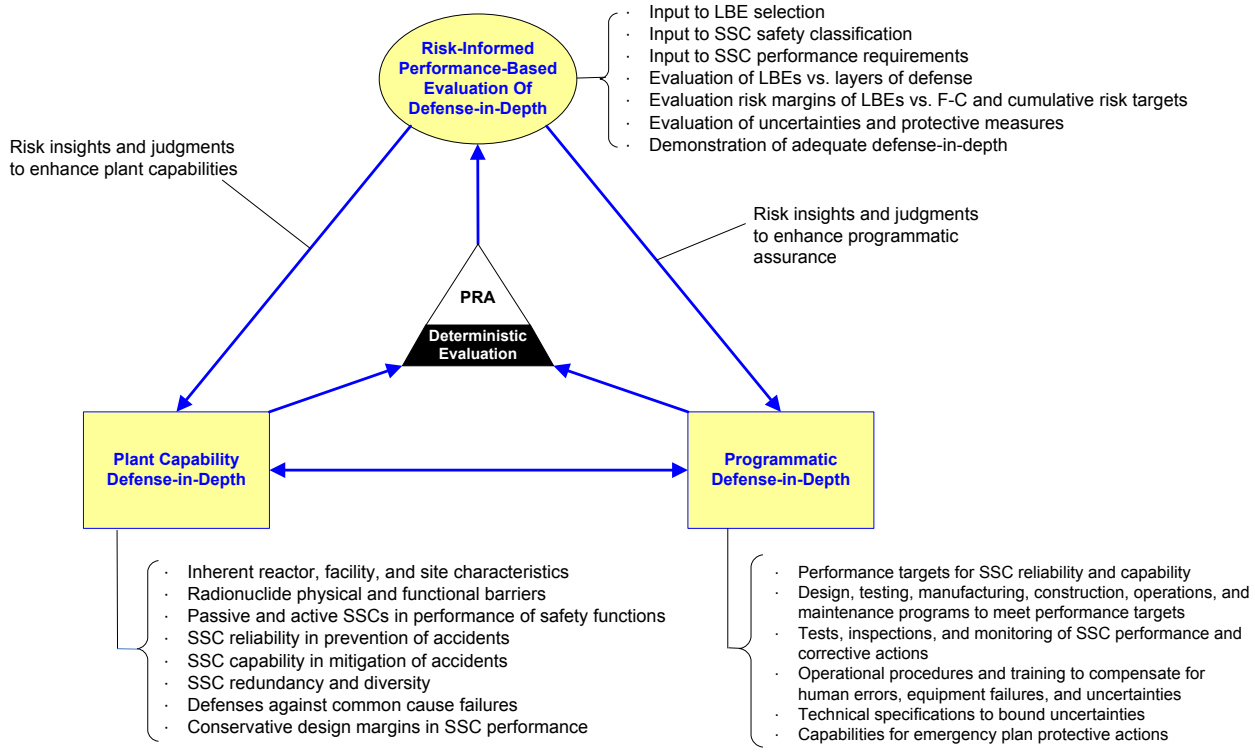
Programmatic Defense-in-Depth

Programmatic DID is used to address uncertainties when evaluating plant capability DID as well as where programmatic protective strategies are defined. It is used to incorporate special treatment[†] during design, manufacturing, constructing, operating, maintaining, testing, and inspecting of the plant and the associated processes to ensure there is reasonable assurance that the predicted performance can be achieved throughout the lifetime of the plant. The use of performance-based measures, where practical, to monitor plant parameters and equipment performance that have a direct connection to risk management and equipment and human reliability are considered essential.

Risk-Informed Evaluation of Defense-in-Depth

This element provides a systematic, holistic, integrated, and transparent process for examining the DID adequacy achieved by the combination of plant capability and programmatic elements. This evaluation is performed by a risk-informed integrated decision-making (RIDM) process to assess and establish whether DID is sufficient and to enable consideration of different alternatives for achieving commensurate safety levels at reduced burdens. The outcome of the RIDM process also establishes a DID baseline for managing risk throughout the plant lifecycle.

Figure 3 - Framework for Establishing DID Adequacy



[†]According to Regulatory Guide 1.201,[0] "…*special treatment* refers to those requirements that provide increased assurance beyond normal industrial practices that structures, systems, and components (SSCs) perform their design-basis functions."

3.1. Defense in Depth Evaluation Attributes

Specific attributes of the three major elements of DID adequacy determination are summarized in Tables 1, 2 and 3. [4].

Table 1- Plant Capability Defense-In-Depth Attributes

Attribute	Evaluation Focus
Initiating Event and Accident Sequence Completeness	PRA Documentation of Initiating Event Selection and Event Sequence Modelling 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 safety functions Passive and Active SSCs performing 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

Table 2 - Programmatic DID Attributes

Attribute	Evaluation Focus
Quality / Reliability	Performance targets for SSC reliability and capability Design, manufacturing, construction, O&M features, or special treatment sufficient to meet performance targets
Compensation for Uncertainties	Compensation for human errors Compensation for mechanical errors Compensation for unknowns (performance variability) Compensation for unknowns (knowledge uncertainty)
Off-Site Response	Emergency response capability

Table 3 - Risk-Informed and Performance-Based Decision-Making Attributes

Attribute	Evaluation Focus
Use of Risk Triplet Beyond PRA	What can go wrong? How likely is it? What are the consequences?
Knowledge Level	Plant Simulation and Modelling of LBEs State of Knowledge Margin to PB Limits
Uncertainty Management	Magnitude and Sources of Uncertainties
Action Refinement	Implementation Practicality and Effectiveness Cost/Risk/Benefit Considerations

3.2 Plant Capability DID Adequacy Evaluations

Additional guidelines for evaluating each of the attributes have been developed in [4]. The Plant Capability guidelines are shown in Table 4.

Table 4- . Guidelines for Establishing the Adequacy of Overall Plant Capability Defense-in-Depth

<table>
<tr><th rowspan="2">Layer[a]</th><th colspan="2">Layer Guideline</th><th colspan="2">Overall Guidelines</th></tr>
<tr><th>Quantitative</th><th>Qualitative</th><th>Quantitative</th><th>Qualitative</th></tr>
<tr><td>1) Prevent off-normal operation and AOOs</td><td colspan="2">Maintain frequency of plant transients within designed cycles; meet user requirements for plant reliability and availability[b]</td><td rowspan="5">Meet F-C target for all LBEs and cumulative risk metric targets with sufficient[d] margins</td><td rowspan="5">No single design or operational feature,[c] no matter how robust, is exclusively relied upon to satisfy the five layers of defense</td></tr>
<tr><td>2) Control abnormal operation, detect failures, and prevent DBEs</td><td>Maintain frequency of all DBEs < 10^{-2}/ plant-year</td><td>Minimize frequency of challenges to safety-related SSCs</td></tr>
<tr><td>3) Control DBEs within the analyzed design basis conditions and prevent BDBEs</td><td>Maintain frequency of all BDBEs < 10^{-4}/ plant-year</td><td>No single design or operational feature[c] relied upon to meet quantitative objective for all DBEs</td></tr>
<tr><td>4) Control severe plant conditions, mitigate consequences of BDBEs</td><td rowspan="2">Maintain individual risks from all LBEs < QHOs with sufficient[d] margins</td><td rowspan="2">No single barrier[c] or plant feature relied upon to limit releases in achieving quantitative objectives for all BDBEs</td></tr>
<tr><td>5) Deploy adequate offsite protective actions and prevent adverse impact on public health and safety</td></tr>
</table>

Notes:

[a] The plant design and operational features and protective strategies employed to support each layer should be functionally independent

[b] Non-regulatory user requirements for plant reliability and availability and design targets for transient cycles should limit the frequency of initiating events and transients and thereby contribute to the protective strategies for this layer of DID. Quantitative and qualitative targets for these parameters are design specific.

[c] This criterion implies no excessive reliance on programmatic activities or human actions and that at least two independent means are provided to meet this objective.

[d] The level of margins between the LBE risks and the QHOs provides objective evidence of the plant capabilities for DID. Sufficiency will be decided by the IDP.

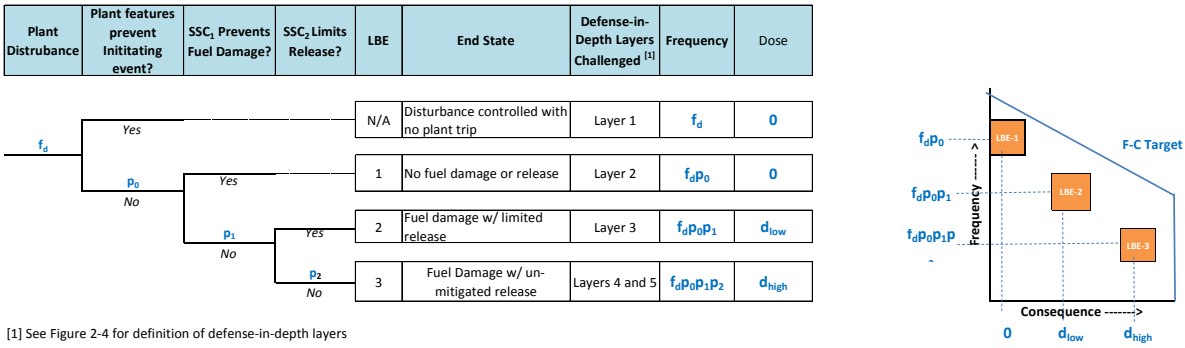
Supporting discussions are provided in [4] for these guidance statements. Similarly, more detailed guidance is provided for Programmatic DID and the integrated Evaluation of DID adequacy. Additionally, for many of the evaluation attributes, a set of questions has been developed to provide the user with an initial means to initiate the evaluation.

Layers of Defense and Prevention and Mitigation Balance

An important consideration in the safety classification of SSCs and in the formulation of SSC performance requirements is the understanding of the roles of SSCs modeled in the PRA in the prevention and mitigation of accidents.[3] This understanding is the basis for the formulation of the SSC capability requirements for mitigation of the challenges represented in the LBEs as well as the reliability requirements to prevent LBEs with more severe consequences. This understanding is also key to recognizing how the plant capabilities for DID achieve an appropriate balance between accident prevention and mitigation across different layers of defense, which permits an examination of the evaluation of the plant capabilities in the context of the layers of defense.

This concept is illustrated in **Error! Reference source not found.Error! Reference source not found.**Figure 4, which presents an event tree with an initial "plant disturbance." The figure reflects the response of the plant in terms of plant features that could prevent the disturbance from creating an initiating event, and two sets of SSCs that have the capability to prevent or mitigate an accident. SSC_1 has the capability to prevent fuel damage, and SSC_2 has the capability to limit the release if fuel damage occurs. The different LBE end states represent different layers of defense in response to the initiating event. The evaluation of DID adequacy uses risk insights into the evaluation of the LBE end states, the frequency of occurrence of adverse end states, the number of layers of defense needed to mitigate the initiating event within the F-C targets, the risk significance of LBE uncertainties on the likely outcomes, and the potential compensatory actions that would materially improve plant performance and/or performance assurance. As shown in the figure, the plant features and SSCs have both prevention and mitigation functions. The prevention metric is the SSC reliability, whereas the mitigation metric is SSC capability.

Figure 4- Evaluating SSC functions in Supporting the Layers of Defense-in-Depth



SSC	LBEs	Function	SSC Performance Attribute for Special Treatment
Plant	N/A	Prevent initiating event	Reliability of plant features preventing initiating event
SSC_1	1	Mitigate initiating event	Capability to prevent fuel damage
	2	Prevent fuel damage	Reliability of mitigation function
	3	Help prevent large release	Reliability of mitigation function
SSC_2	2	Mitigate fuel damage	Capability to limit release from fuel damage
	3	Prevent unmitigated release	Reliability of mitigation function

Evaluation of LBE and Plant Risk Margins

The evaluation of LBE outcomes is done in two ways, the margins to the F-C target are measured based on mean values of the LBE frequencies and doses; and, A more conservative evaluation of margins in which the 95th percentile upper bound values for both LBE frequency and dose are used to calculate the margins. At the plant level, cumulative LBE outcomes are compared to established cumulative risk objectives. A more complete discussion can be found in [1]

3.3 Programmatic DID Adequacy Evaluations

The adequacy of programmatic DID is based on meeting the following objectives:

- Assuring adequate margins exist between the assessed LBE risks relative to the F-C target including quantified uncertainties

- Assuring adequate margins exist between the assessed total plant risks relative to the Cumulative Risk Targets
- Assuring appropriate targets for SSC reliability and performance capability are reflected in design and operational programs for each LBE
- Providing adequate assurance that the risk, reliability, and performance targets will be met and maintained throughout the life of the plant with adequate consideration of sources of significant uncertainties

Unlike the plant capabilities for DID which can be described in physical terms and are amenable to quantitative evaluation, the programmatic DID adequacy must be established using engineering judgment by determining what package of DID attributes are sufficient to meet the above objectives. These judgments are made by the IDP using the programmatic DID attributes and evaluation considerations in **Error! Reference source not found.Error! Reference source not found.**Table 2 above and Table 5 below. As can be seen from the Evaluation Considerations, a greater use of judgement is employed in evaluating Programmatic DID attributes. This is driven by the need to systematically evaluate the different sources of uncertainties in a design using risk insights available to moderate the chosen actions to those that have meaningful impacts on the performance-based objectives of the process.

Table 5 - Evaluation Considerations for Evaluating Programmatic DID Attributes

Attribute	Evaluation Focus	Implementation Strategies	Evaluation Considerations
Quality / Reliability	Design Testing Manufacturing Construction O&M	Conservatism with Bias to Prevention Equipment Codes and Standards Equipment Qualification Performance Testing Graded QA	1. Is there appropriate bias to prevention of AOOs progressing to postulated accidents? 2. Has appropriate conservatism been applied in bounding deterministic safety analysis of more risk significant LBEs? 3. Is there reasonable agreement between the deterministic safety analysis of DBAs and the upper bound consequences of the corresponding risk-informed DBE included in the LBE set? 4. Have the most limiting design conditions for SSCs in plant safety and risk analysis been used for selection of safety–related SSC design criteria? 5. Is the reliability of functions within systems relied on for safety overly dependent on a single inherent or passive feature for risk significant LBEs? 6. Is the reliability of active functions relied upon in risk significant LBEs achieved with appropriate redundancy or diversity within a layer of defense? 7. Have the identified safety-related SSCs been properly classified for special treatment consistent with their risk significance?

Attribute	Evaluation Focus	Implementation Strategies	Evaluation Considerations
Compensation for Uncertainties	Compensation for Human Errors	Operational Command and Control Practices Training and Qualification Plant Simulators Independent Oversight and Inspection Programs Reactor Oversight Program	1. Have the insights from the Human Factors Engineering program been included in the PRA appropriately? 2. Have plant system control designs minimized the reliance on human performance as part of risk-significant LBE scenarios? 3. Have plant protection functions been automated with highly reliable systems for all DBAs? 4. Are there adequate indications of plant state and transient performance for operators to effectively monitor all risk-significant LBEs? 5. Are the risk-significant LBEs all properly modeled on the plant reference simulator and adequately confirmed by deterministic safety analysis? 6. Are all LBEs for all modes and states capable of being demonstrated on the plant reference simulator for training purposes?
	Compensation for Mechanical Errors	Operational Technical Specifications Allowable Outage Times Part 21 Reporting Maintenance Rule Scope	1. Are all risk-significant LBE limiting condition for operation reflected in plant Operating Technical Specifications? 2. Are Allowable Outage Times in Technical Specifications consistent with assumed functional reliability levels for risk-significant LBEs? 3. Are all risk-significant SSCs properly included in the Maintenance Program?
	Compensation for Unknowns (Performance Variability)	Operational Technical Specifications In-Service Monitoring Programs	1. Are the Technical Specification for risk-significant SSCs consistent with achieving the necessary safety function outcomes for the risk significant LBEs? 2. Are the in-service monitoring programs aligned with the risk-significant SSC identified through the RIPB SSC Classification process?
	Compensation for Unknowns (Knowledge Uncertainty)	Site Selection PIRT/ Technical Readiness Levels Integral Systems Tests / Separate Effects Tests	1. Have the uncertainties identified in PIRT or similar evaluation processes been satisfactorily addressed with respect to their impact on plant capability and associated safety analyses? 2. Has physical testing been done to confirm risk significant SSC performance within the assumed bounds of the risk and safety assessments? 3. Have plant siting requirements been conservatively established based on the risk from severe accidents identified in the PRA? 4. Has the PRA been peer reviewed in accordance with applicable industry standards and regulatory guidance? 5. Are hazards not included in the PRA low risk to the public based on bounding deterministic analysis?
Off-Site Response	Emergency Response Capability	Layers of Response Strategies EPZ location EP Programs Public Notification Capability	1. Are functional response features appropriately considered in the design and emergency operational response capabilities for severe events as a means of providing additional DID for undefined event conditions? 2. Is the Emergency Planning Zone appropriate for the full set of DBEs and BDBEs identified in the LBE selection process? 3. Is the time sufficient to execute EP protective actions for risk significant LBEs consistent with the event timelines in the LBEs?

3.4 RIPB Integrated Evaluation of DID Adequacy

An Integrated Decision Panel (IDP)should be responsible for evaluating the adequacy of DID. Its makeup should be cross-functional. For currently operating plants that are employing risk-informed changes to the licensing basis, such as risk-informed safety classification under 10 CFR 50.69, such panels are employed to guide the risk-informed decision-making process. Similar methods can be effectively established within a design environment [1,2,4]. The DID attributes shown in Table 3 above reflect the importance of confirming the overall outcomes of the design are capable of being achieved in a robust and comprehensive way in the bright light of uncertainties and margins associated with the plant and the means to manage residual risks throughout the operational life.

The RIPB-DM process should include the following steps regardless of the phase of design:

- Identification of the DID issue to be decided
- Identification of the combination of defined DID attributes important to address current issues
- Comprehensive consideration of each of the defined attributes individually, incorporating insights from deterministic analyses, probabilistic insights, operating experience, engineering judgment, etc.
- Knowledgeable, responsible individuals make a collaborative decision based on the defined attribute evaluation requirements
- If compensatory actions are needed, identification of potential plant capability and /or programmatic choices
- Implementation closure of DID open actions and documentation of the results of the RIPB-DM process and rationale for their decisions in a record appropriate for the stage of the design process.

Compensatory Action Adequacy

DID adequacy evaluations should include the necessity, scope and sufficiency of existing design and operational programs being applied to a design or portion of a design. Specific consideration should be given to the RIPB capabilities of each program type to provide meaningful contributions to risk reduction or performance assurance based on the risk significance of SSCs associated with each LBE. Particular attention should be paid to the number of layers of defense that are associated with initiating events that can progressively cascade to the point of challenging public safety objectives. Initiating events that cannot cascade to a point of threating public health should be found acceptable with fewer layers of defense than events that have the potential to release large amounts of radiation.

For risk significant BDBE, the evaluation should take into account both the magnitude of the consequences and the time frame for actions in determining the need for or choice of compensatory actions. Where dose predictions fall below regulatory limits, the availability of programmatic actions to mitigate those events should be considered over more sweeping changes to plant design to eliminate the BDBE which could be impractical to implement or excessively burdensome. Small changes to the design that improve the likelihood of successful actions should be consider in the light of the stage of design development attained. For any BDBE that exceeds regulatory siting limits, if practical, design changes should be considered over reliance on EP DID alone.

DID Evaluation Baselines

Like many other licensing basis topics, changes in physical, functional, operational, or programmatic features require consideration of the potential for reduction of DID before proceeding. This requires that a current baseline for DID be available as a reference for change evaluation. These changes in turn require revisions to the PRA and all the subsequent steps in the integrated design process. The baseline DID evaluation will be documented in sufficient detail so it can be efficiently updated in future design development or operational phase iterations. The baseline documentation is essential for completing operating phase change safety assessments for criteria in 10CFR50.59 or similar regulatory requirements. The checklists developed in [4] can serve as a reminder as to the scope of the most recent integrated evaluation. The DID baseline should be maintained in a controlled document.

4. CONCLUSION

This approach establishes a means to systematically evaluate Defense in Depth adequacy. It utilizes modern PRA methods to assure a robust set of RIPB LBE are established; the underlying SSCs are properly classified consistent with their risk significance, design margins for SSCs and plant performance are sufficient including RIPB uncertainties, that the design is robust, ie, adequately considers uncertainties of all types that materially contribute to the understanding the range of performance expected from the plant; and, that meaningful programmatic activities are established to provide additional assurance that the predicted performance is sustained throughout the plant life.

Acknowledgements

This work has benefited from the commitment of Southern Company Services and the U.S. Department of Energy to continue work envisioned by earlier pioneers and leaders who believed in the promise of well structured, risk-informed and performance-based practices needed for advanced reactors.

References

[1] Idaho National Laboratory, "Modernization of Technical Requirements for Licensing of Advanced Non-Light Water Reactors, Selection of Licensing Basis Events," Draft, April 2017. [Adams Accession Number ML17104A254]

[2] Idaho National Laboratory, "Modernization of Technical Requirements for Licensing of Advanced Non-Light Water Reactors, Probabilistic Risk Assessment Approach," Draft, June 2017. [Adams Accession Number ML17158B543]

[3] Idaho National Laboratory, "Modernization of Technical Requirements for Licensing of Advanced Non-Light Water Reactors, Safety Classification and Performance Criteria for Structures, Systems and Components," Draft, October 2017. [Adams accession number ML17290A463]

[4] Idaho National Laboratory, "Modernization of Technical Requirements for Licensing of Advanced Non-Light Water Reactors, Risk-Informed and Performance-Based Evaluation of Defense-in-Depth Adequacy," Draft, December 2017. [Adams accession number ML17290A463]

[5] US Nuclear Regulatory Commission, Glossary https://www.nrc.gov/reading-rm/basic-ref/glossary/defense-in-depth.html

[6] US Nuclear Regulatory Commission, "Historical Review and Observations of Defense-in-Depth (NUREG/KM-0009)" April 2016

[7] International Atomic Energy Agency, Safety Report Series No. 46, "Assessment of Defense in Depth for Nuclear Power Plants," 2005.

[8] Regulatory Guide 1.201 (For Trial Use), "Guidelines for Categorizing Structures, Systems, and Components in Nuclear Power Plants According to Their Safety Significance," Revision 1, May 2006.