

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



**Edward G Wallace<sup>a</sup>, Karl Fleming<sup>b</sup>, and Amir Afzali<sup>c</sup>**

---

<sup>a</sup> GNBC Associates, Inc., Denver, CO, USA\*

<sup>b</sup> KNF Consulting Services LLC, Spokane, WA, USA

<sup>c</sup> Southern Company Services, Birmingham, AL, USA

Presented to

PSAM-14

Los Angeles, CA September 20, 2018

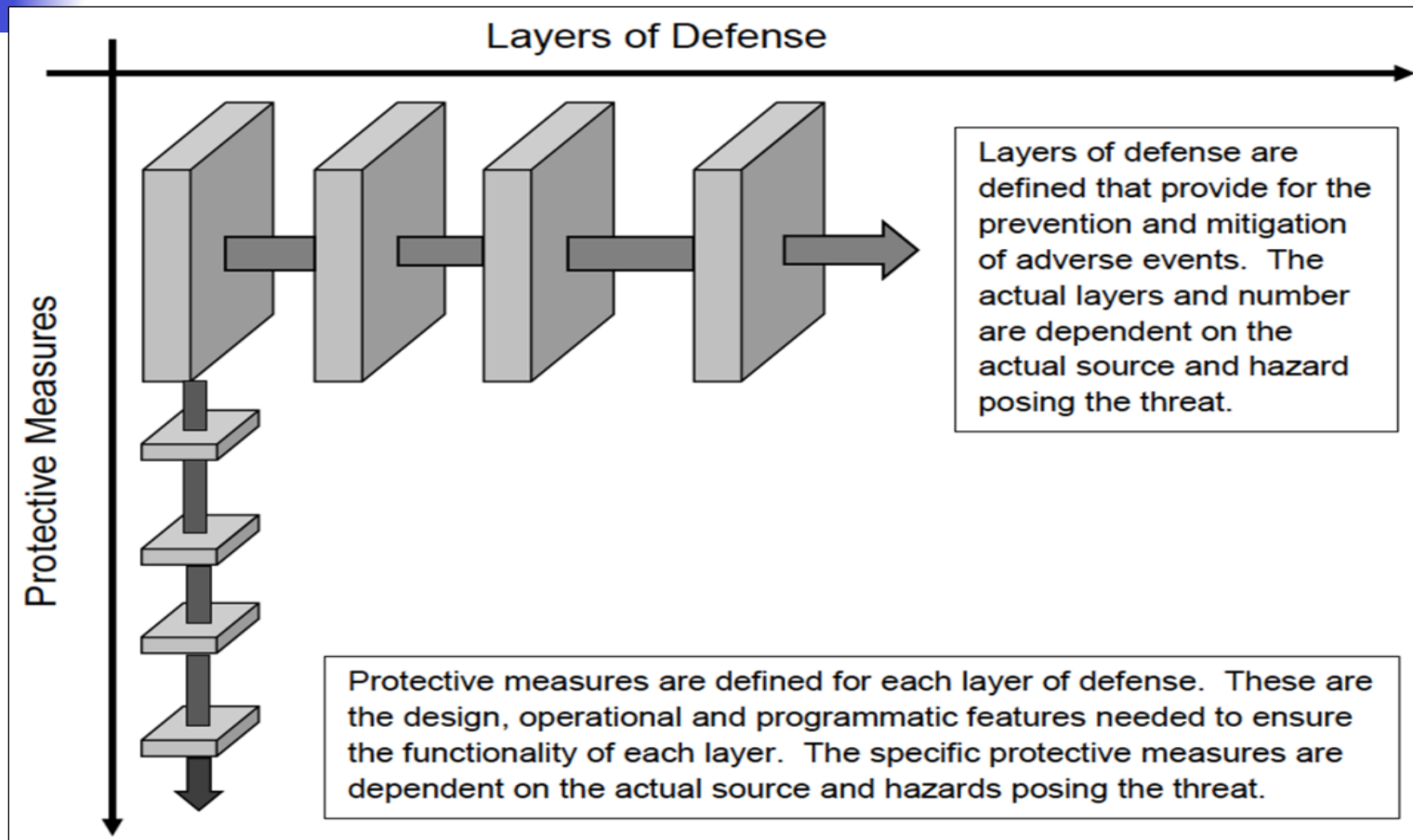


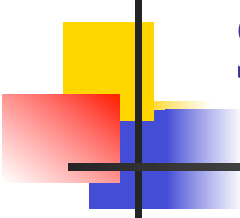
# NRC Defense in Depth Philosophy

---

“...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.”

# NRC Defense-in-Depth Concept





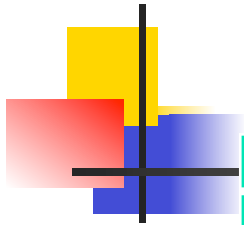
# LMP DID Adequacy Evaluation – Specific Objectives

---

- 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 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.**
- **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**
- Identify the importance of defenses against common cause failures and need to minimize dependencies among the layers of defense
- Present guidelines for evaluating and establishing a DID adequacy baseline
- Achieve agreement on how DID adequacy is achieved among those responsible for designing, operating, reviewing, and licensing advanced non-LWRs

# LMP Defense In Depth Adequacy Structure

---



# Plant Capability DID Attributes

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



# Programmatic DID Attributes

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



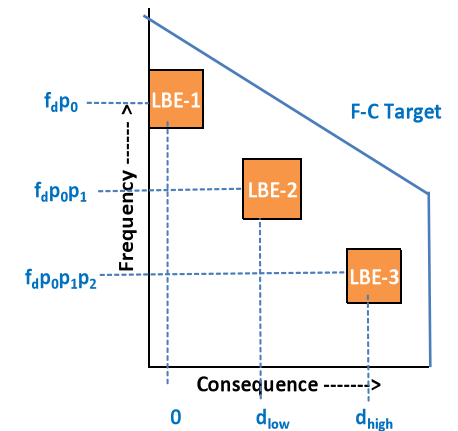
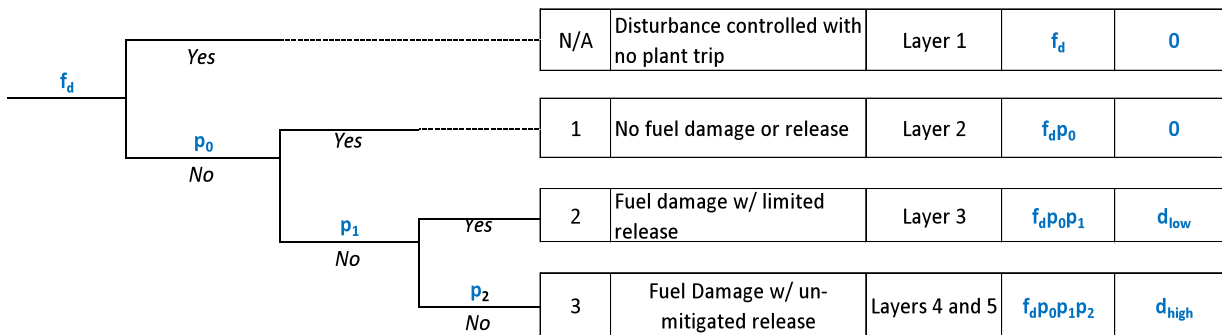
# RIPB Decision-Making Attributes

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



# SSC Layers of Defense Capability and Reliability in Prevention and Mitigation of Accidents

Plant Disturbance	Plant features prevent Initiating event?	SSC <sub>1</sub> Prevents Fuel Damage?	SSC <sub>2</sub> Limits Release?	LBE	End State	Defense-in-Depth Layers Challenged <sup>[1]</sup>	Frequency	Dose
-------------------	------------------------------------------	----------------------------------------	----------------------------------	-----	-----------	---------------------------------------------------	-----------	------

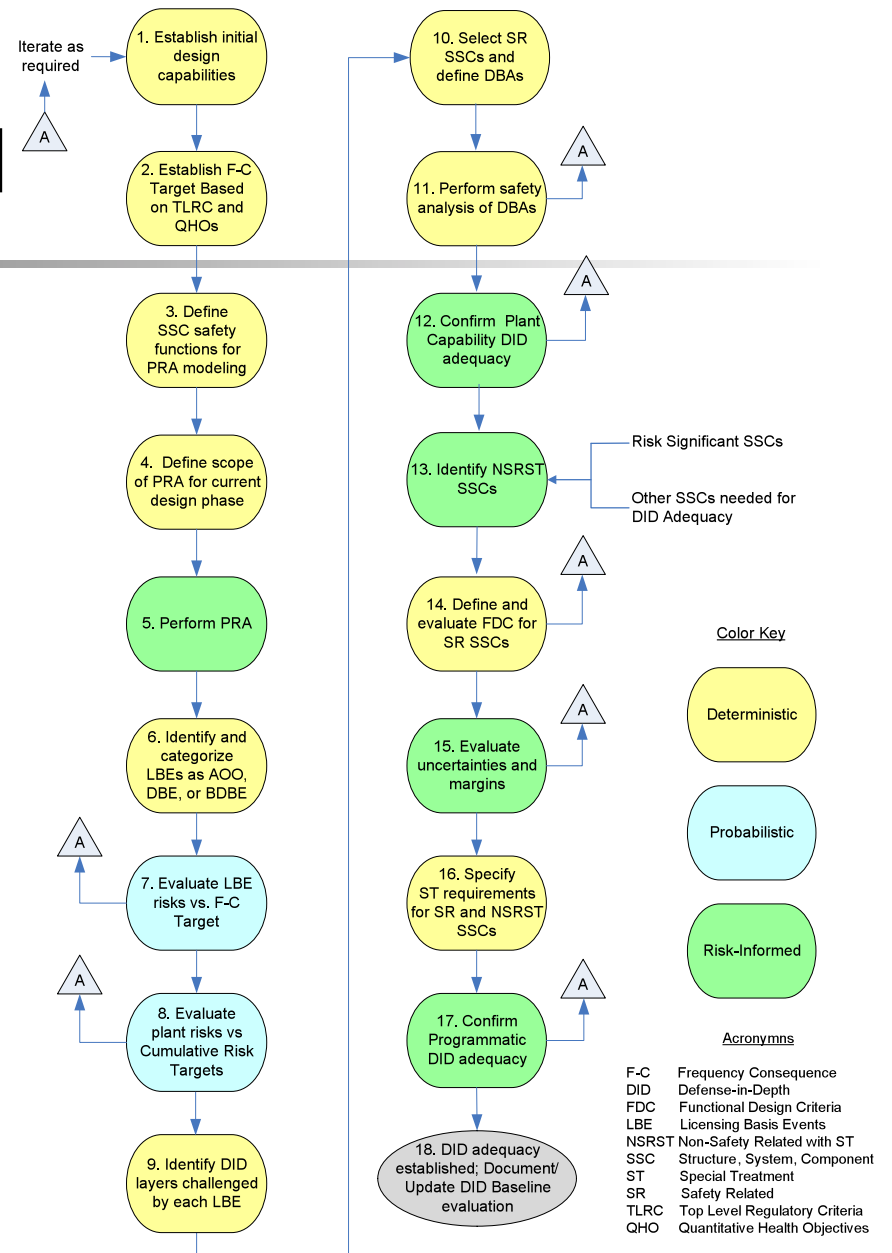


[1] See Figure 2-4 for definition of defense-in-depth layers

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

# Integrated Process for Incorporation and Evaluation of DID

- Tasks are not necessarily sequential
- Tasks can begin early in the conceptual design process and mature with the design evolution
- All of the attributes included in the DID adequacy evaluation are completed when the design baseline for the license application is submitted
- Programmatic confirmation of performance and sustained DID continues for life of the plant.





# Special Considerations Overview

---

- Metrics
  - LBE Metrics
  - SSC Metrics
- Margins
  - Plant performance margins (LBEs)
  - SSC design performance conservatism
- Uncertainties
  - Completeness
  - Analyzed Uncertainties
  - Residual Risks
- Compensatory Action Decisions
  - Choices
  - Impact on Risk
  - Timing
  - Practicality



# Uncertainties

---

## ■ Completeness

- PRA completeness for identified hazards
- Sources of risk-significant uncertainties
- Treatment of radiological and other hazards not included in PRA

## ■ Analyzed

- Data Availability
- Model Maturity
- Performance History

## ■ Residual Risks

- Emergency Planning Zone basis
- Emergency Plan response effectiveness
- Operational Technical Specifications Completeness
- Allowable Outage Times basis
- Monitoring of Plant Long Term Performance
- Etc.