Modernization of Technical Requirements for Licensing of Advanced Non-Light Water Reactors

Risk-Informed and Performance-Based Evaluation of Defense-in-Depth Adequacy

Draft Report Revision A
Issued for Collaborative Review

Document Number
SC-xxx Rev A

December 2017

Prepared for:
U.S. Department of Energy (DOE)
Office of Nuclear Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

Modernization of Technical Requirements for Licensing of Advanced Non-Light Water Reactors

Risk-Informed and Performance-Based Evaluation of Defense-in-Depth Adequacy

Draft Report Revision A
Issued for Collaborative Review

Document Number
SC-xxx Rev A

December 2017

Issued for Collaborative Review by:

_____ _____

Amir Afzali, Next Generation Licensing and Policy Director Date
Southern Company Services

Disclaimer

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States (U.S.) Government nor any agency thereof, nor any of their employees, nor Southern Company Services, Inc., nor any of its employees, nor any of its subcontractors, nor any of its sponsors or co-funders, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

Abstract

This document proposes a framework and associated guidelines for establishing, then evaluating, confirming, and documenting, the adequacy of defense-in-depth (DID) for advanced non-light water reactor technologies. It was developed as part of the Licensing Modernization Project (LMP) led by Southern Company and cost-shared by the U.S. Department of Energy. The proposed framework, which converts the DID philosophy into a process that is implementable, embraces existing U.S. and international definitions and philosophies of DID that set the foundation for the approach, and it builds on the DID framework developed in the U.S. Department of Energy Next Generation Nuclear Plant project.

The proposed DID framework 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.

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, selection of Licensing Basis Events (LBEs), safety classification of Structures, Systems, and Components (SSCs), and specification of performance requirements for SSCs. 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 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.

The focus of this paper is assurance of DID adequacy with respect to protection of the public from radiological exposures resulting from accidental releases of radioactive material. While other hazards are not specifically addressed, this framework is expected to be beneficial for determining DID adequacy for them as well.

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 necessary to provide reasonable assurance of adequate protection. When implemented, the LMP DID framework provides a more objective means to answer the question for a specific design: "When is enough, enough?"

Table of Contents

List of Figures

List of Tables

List of Abbreviations

ANS	American Nuclear Society
AOO	Anticipated Operational Occurrence
ASME	American Society of Mechanical Engineers
BDBE*	Beyond Design Basis Event
CFR	Code of Federal Regulations
DBA	Design Basis Accident
DBE*	Design Basis Event
DID	defense-in-depth
DOE	Department of Energy
F-C	Frequency-Consequence
FDC	Functional Design Criteria
HPB	Helium Pressure Boundary
IAEA	International Atomic Energy Agency
IDP	Integrated Decision Panel
IE	Initiating Event
LBE*	Licensing Basis Event
LMP	Licensing Modernization Project
MHTGR	a specific modular high temperature gas-cooled reactor designed by General Atomics
NEI	Nuclear Energy Institute
non-LWR	non-light water reactor
NSRST	Non-Safety-Related with Special Treatment
NST	Non-Safety-Related with No Special Treatment
NGNP	Next Generation Nuclear Plant
NRC	Nuclear Regulatory Commission
O&M	Operations and Maintenance
PRA	Probabilistic Risk Assessment
QHO	Quantitative Health Objective
RCCS	Reactor Cavity Cooling System
RIDM	risk-informed integrated decision-making
RIPB-DM	risk-informed and performance-based integrated decision-making
SR	Safety-Related
SSC	Structures, Systems, and Components
TI-RIPB	technology-inclusive, risk-informed, and performance-based
TLRC	Top Level Regulatory Criteria
US	United States

*These terms have special meanings defined in this document.

1.0 INTRODUCTION

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. What is included in the Licensing Modernization Project (LMP) is an approach that permits the establishment of DID in design, construction, maintenance, and operation of nuclear facilities. This is accomplished by the reactor designer and operator with the objective of getting agreement that adequate DID has been achieved. Achievement of DID occurs when all stakeholders (designers, license applicants, regulators, etc.) make clear and consistent decisions regarding DID adequacy. DID should be integral to the overall design process and not simply "bolted on" or applied as an appendage at design completion to compensate for inadequate design choices made across the duration of the design process.

The LMP 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 proposed LMP framework for establishing and evaluating DID adequacy for advanced non-light water reactors (non-LWRs) builds on the DID framework proposed for the Next Generation Nuclear Plant (NGNP) project[1] which in turn benefitted from earlier efforts for the Exelon Pebble Bed Modular Reactor[2] and American Nuclear Society (ANS) 53.1[3] to define a technology-inclusive framework for evaluating DID.

Establishing DID adequacy involves incorporating DID design features, operating and emergency procedures and other programmatic elements. DID adequacy is evaluated by using a series of RIPB decisions regarding design, plant risk assessment, selection and evaluation of licensing basis events, safety classification of Structures, Systems, and Components (SSCs), specification of performance requirements for SSCs, and programs to ensure these performance requirements are maintained throughout the life of the plant.

1.1 Purpose

The purpose of this document is to define the LMP framework for establishing and evaluating DID that employs a technology-inclusive, risk-informed, and performance-based (TI-RIPB) process. This process includes an approach for the incorporation of DID protective measures into the plant design and a method for the evaluation of DID adequacy. The framework is based on the premise that DID is an integral part of the design which is implemented in a manner that satisfies a set of DID attributes. These attributes include a set of plant capabilities and complementary programmatic measures that are necessary to assure that the plant performs within acceptable public risks for the lifetime of the plant with adequate margins for uncertainties.

When the framework described in this document is applied, the user will have sufficient information to make a structured and reproducible judgment about the adequacy of the DID provisions. This information will include:

- 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

1.2 Objective

The objectives of this document are to:

- 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. These DID attributes are reflected in the design features of the plant and the reliabilities and capabilities of SSCs, including fission product barriers[*] that contribute to multiple, functionally independent layers of defense, in the prevention and mitigation of accidents and the prevention of adverse effects on public health and safety.

[*]In this paper, the term "barrier" is used to denote any plant feature that is responsible to either full or partial reduction of the quantity of radionuclide material that may be released during an LBE. It includes features such as physical or functional barriers or any feature that is responsible as part of a layer of defense for mitigating the quantity of material released from the plant including time delays during fission product transport that permit radionuclide decay or provide extended response times for alternative 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
- 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

1.3 Relationship to Other LMP Documents

The DID evaluation framework described in this paper is intended to be used in conjunction with other aspects of the LMP framework described in the supporting papers outlined below.

Probabilistic Rick Assessment (PRA) Approach

The PRA approach document describes a technology-inclusive approach for developing a PRA for an advanced non-LWR to support the design and provide risk insights for the selection of Licensing Basis Events (LBEs), safety classification of SSCs, and risk-informed evaluation of DID. The PRA is an important input to the selection of LBEs and provides a basis for describing layers of defense, establishing the risk significance of LBEs and SSCs, and identifying sources of uncertainty that must be addressed to achieve DID adequacy. The current paper discusses how uncertainties exposed by the PRA are evaluated in the DID process to identify protective strategies for compensating for uncertainties.

Selection of Licensing Basis Events

Key inputs to the selection of LBEs are derived from a PRA of an advanced non-LWR plant. These inputs together with deterministic inputs e.g., design selections, selection of safety-related SSCs, are used as part of the selection and evaluation of LBEs. As part of the LBE selection and evaluation process described in the LBE document, the engineering and safety analysis effort will result in a selection of a set of safety-related SSCs that are necessary and sufficient to perform the safety functions required to keep the Design Basis Events (DBEs) within the Frequency-Consequence (F-C) target, and to prevent any high consequence Beyond Design Basis Event (BDBE) from migrating into the DBE region and exceeding the F-C target.

The safety-related SSCs are then relied upon to mitigate all the Design Basis Accidents (DBAs) within the dose limits of 10 CFR 50.34 using conservative assumptions. This DID paper describes how LBEs are reviewed to identify the layers of defense in the design, to evaluate margins against risk targets, to evaluate uncertainties in the risk evaluation, and to set performance targets for plant reliability and capability which comprise important elements of programmatic defense-in-depth.

Safety Classification and Performance Criteria for SSCs

The SSC document describes the LMP approach for the safety classification of SSCs, selection of functional design criteria for safety-related SSCs, and the selection of performance requirements for SSC reliability and capability, with special treatment for safety significant SSCs. The current paper covers how DID attributes are reflected in the selection of these performance requirements and the monitoring of performance against these requirements.

2.0 LMP FRAMEWORK FOR ESTABLISHING ADEQUACY OF DID

2.1 Objectives for DID Evaluation Process

Consistent with LMP papers on PRA approach, LBE selection and evaluation, and SSC safety classification, a set of objectives was identified for the evaluation process for DID adequacy. To meet the objectives of the LMP, the approach to establishing DID adequacy, when fully implemented, should have the characteristics described below.

Systematic and Reproducible

In principle, application of the process by different persons given the same inputs would yield a reasonably comparable level of safety and evaluation of DID adequacy. Any variations should only result from different states of knowledge that are fed into the process.

Sufficiently Complete

The DID adequacy achievement and evaluation process should be capable of defining a sufficiently complete set of DID attributes that assure DID adequacy. These attributes include plant capabilities for preventing and mitigating accidents and programmatic elements to ensure the plant capabilities are realized and maintained for the life of the plant.

Available for Timely Input to Design Decisions

Importantly, the DID adequacy achievement and evaluation process should recognize that design, engineering, construction, and operational decisions that are necessary to implement DID measures are made at an early stage of design and long before the licensing application is prepared. The level of completeness will necessarily grow as the design matures and site characteristics are defined.

Risk-Informed and Performance-Based

The DID adequacy achievement and evaluation process should be risk-informed and performance-based consistent with LMP objectives. Risk-informed, as contrasted with risk-based, means that the process will include an appropriate balance of deterministic and probabilistic elements. Performance-based means that the process will include measurable and quantifiable plant and SSC performance metrics and will be consistent with NRC policies on use of performance-based alternatives.[8]

Reactor Technology-Inclusive

When applying the process to different advanced non-LWRs having fundamentally different safety designs, the approach will yield a transparent establishment and evaluation of DID adequacy that is consistent and effective with respect to assuring public safety outcomes.

Compatible with Applicable Regulatory Requirements

The DID adequacy achievement and evaluation process must account for the current regulatory performance-based requirements with due regard to their prescriptive applicability to advanced non-LWR technologies and associated safety design approaches. The process aligns the generic safety objectives in the regulatory framework with a more structured analysis of the risks of each design. The combination of RIPB insights and systematic examination of uncertainties builds

the foundation for comparison to existing regulatory requirements and the focused application of programmatic features to adequately assure public risk objectives.

2.2 Defense-in-Depth Philosophy

According to the NRC glossary,[1] 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.*

Figure 2-1 provides a graphic that describes the concept of layers of defense embodied in this philosophy taken from NUREG/KM-0009.[5] How this framework is intended for use by operating reactors to evaluate the preservation of DID for risk-informed decisions involving changes to the licensing basis for operating plants is discussed in Reference [6]. As discussed more fully in Reference [5], this framework is consistent with the "levels of defense" concept advanced by the IAEA in Reference [7].

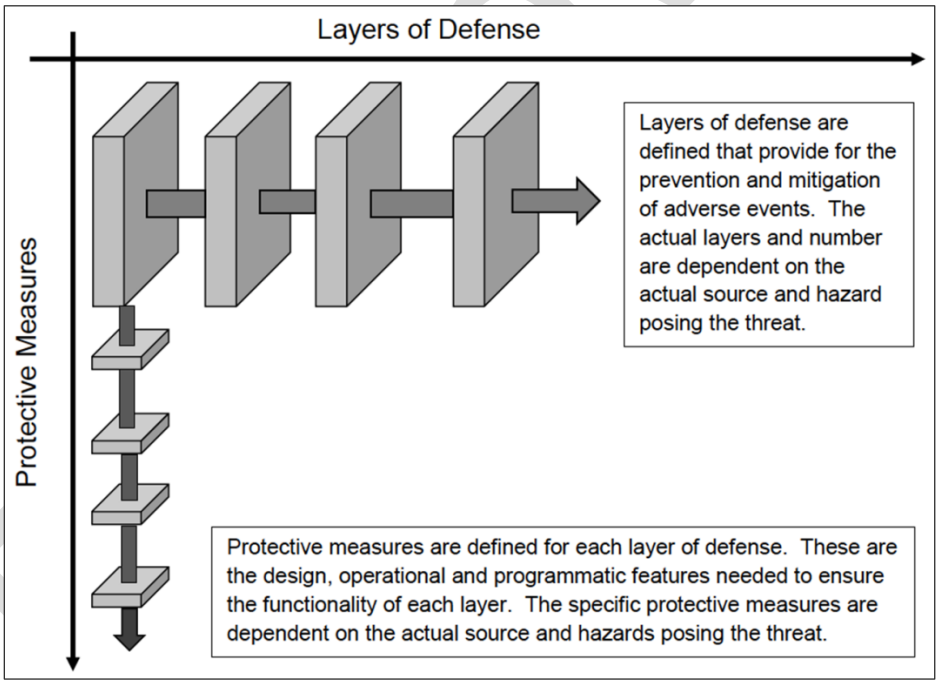


Figure 2-1. U.S. Nuclear Regulatory Commission's Defense-in-Depth Concept[5]

The LMP framework for establishing DID adequacy embraces this layer of defense concept and uses these layers to identify and evaluate DID attributes for establishing DID adequacy.

2.3 NGNP Defense-in-Depth Framework

The LMP framework for establishing DID adequacy builds on the DID framework that was developed for the NGNP project[1] and was incorporated into the ANS Design Standard for Modular Helium Cooled Reactors.[3] Although this framework (was developed for use with high temperature gas cooled reactors, it was developed on a reactor-technology neutral basis. The NGNP DID framework is illustrated in Figure 2-2. The three major process elements are summarized below.

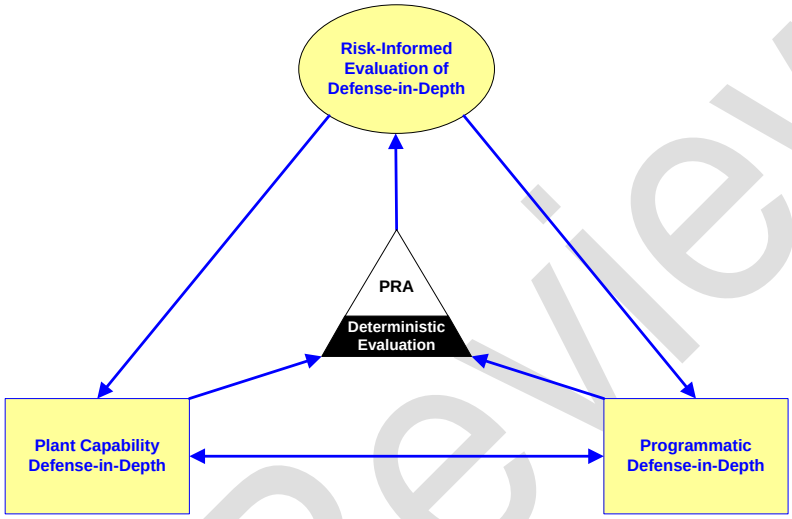


Figure 2-2. NGNP Defense-in-Depth Framework[1]

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 adequate protection. 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 for reasonable assurance of adequate protection achievement 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.

2.4 LMP Framework for Establishing DID Adequacy

The LMP framework for evaluation of DID adequacy is outlined in Figure 2-3.

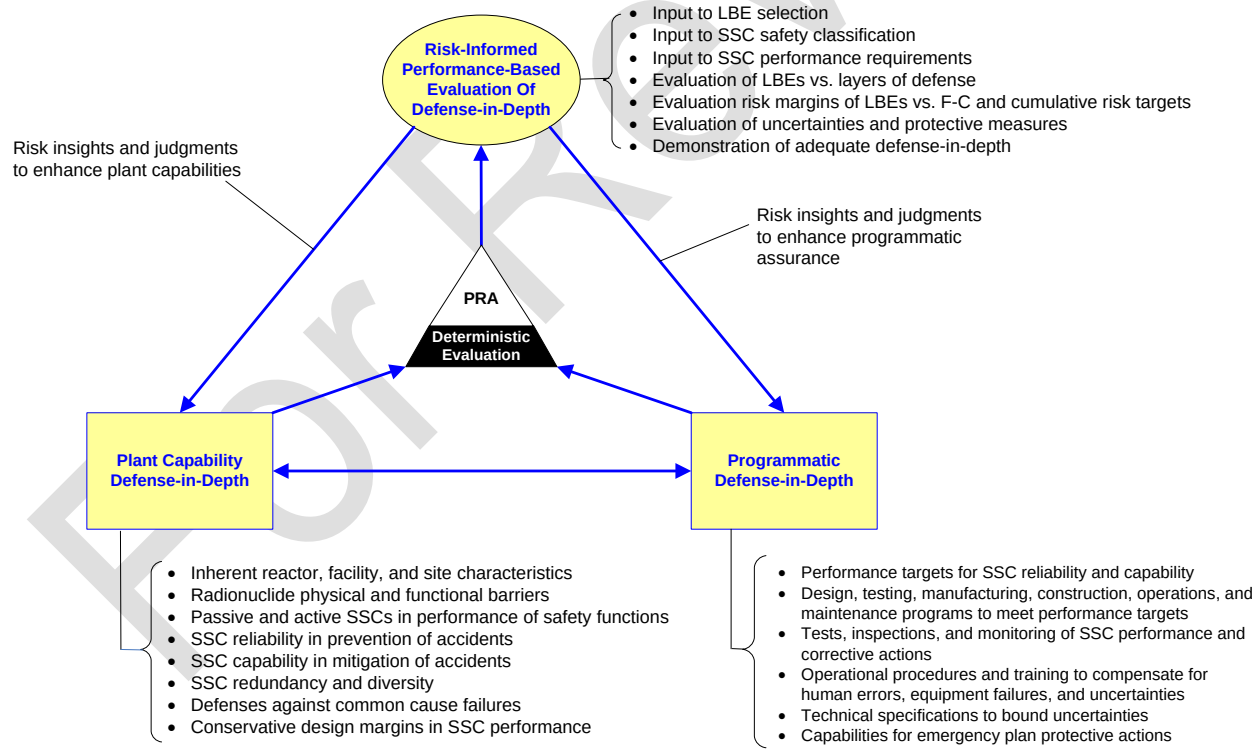


Figure 2-3. LMP Framework for Establishing DID Adequacy

*According to Regulatory Guide 1.201,[17] "…*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."

While there is general alignment with the NGNP framework, the following enhancements are reflected in this version of the framework:

- It is clarified in this version that the evaluation of DID adequacy is both risk-informed and performance-based. This helps to identify important links to the performance requirements that are derived in the LMP framework to LBE selection[9] and evaluation and SSC safety classification[11] approaches.
- The layers of defense and DID attributes of the NRC and IAEA frameworks are more visibly represented.
- The description of DID attributes for plant capability and programmatic DID have been enhanced for consistency with the measures defined in this paper.
- The LMP process for using the layers of defense for performing the RIPB evaluation of plant capabilities and programs, which has been adapted from the IAEA "levels of defense" approach is shown in Figure 2-4. This process is used to evaluate each LBE and to identify the DID attributes that have been incorporated into the design to prevent and mitigate accident sequences and to ensure that they reflect adequate SSC reliability and capability. Those LBEs with the highest levels of risk significance are given greater attention in the evaluation process.

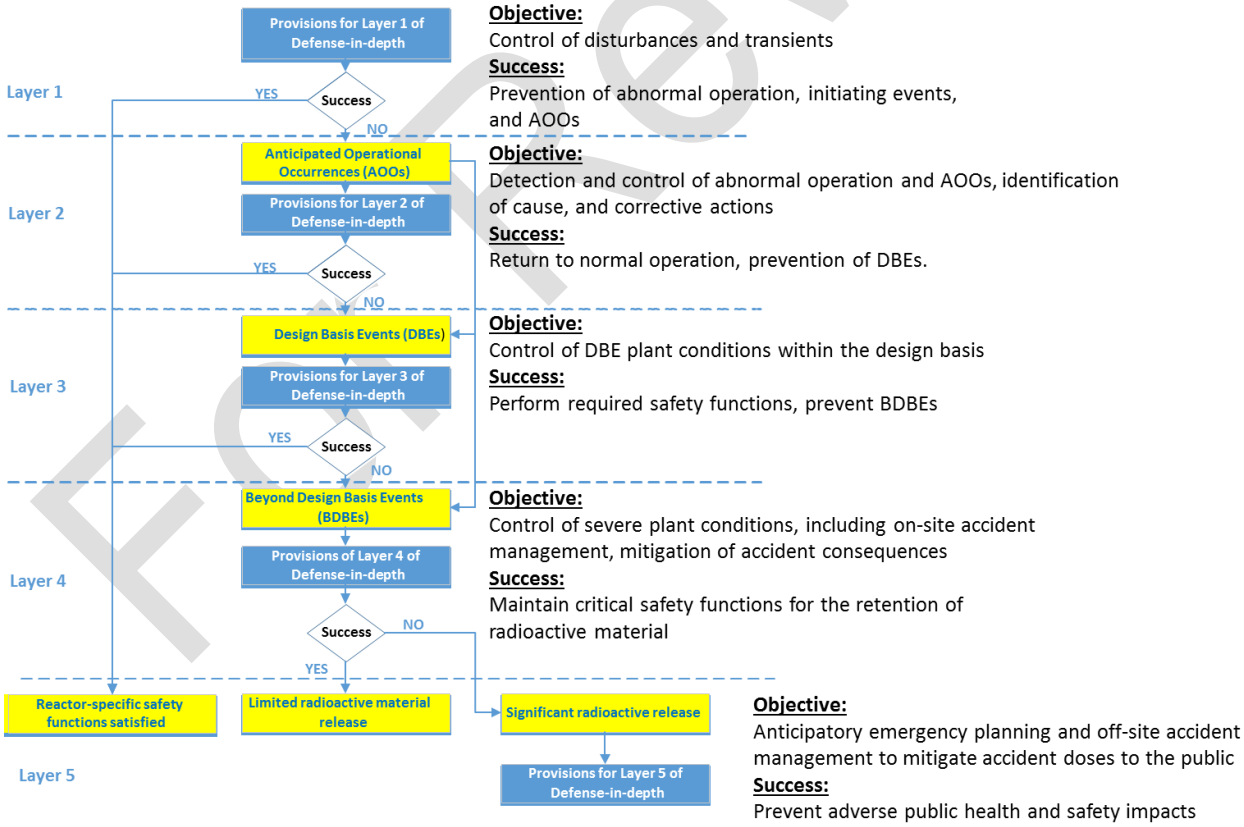


Figure 2-4. LMP Process for Evaluating LBEs Using Layers of Defense Concept Adapted from IAEA[7]

- As explained more fully in the supporting LMP papers on PRA development, LBE selection and evaluation, and SSC safety classification, the PRA is used together with traditional deterministic safety approaches to affect a risk-informed process as shown in the center of Figure 2-3. The PRA is not employed simply to calculate numerical risk metrics, but rather to develop risk insights into the design and to identify sources of uncertainty in the PRA models and supporting data that complement the deterministic elements of the framework. The DID evaluation includes the identification of compensating protective measures to address the risk significant sources of uncertainty so identified.

2.5 LMP Integrated Framework for Incorporation and Evaluation of DID

DID is incorporated into all phases of defining the design requirements, developing the design, evaluating the design from both deterministic and probabilistic perspectives, and defining the programs to ensure adequate protection. The reactor designer is responsible for ensuring that DID is achieved through the incorporation of DID features and programs in the design phases and in turn, conducting the evaluation that arrives at the decision of whether adequate DID has been achieved. The reactor designer implements these responsibilities through the formation of an Integrated Decision Panel (IDP) which guides the overall design effort (including development of plant capability and programmatic DID features), conducts the DID adequacy evaluation of that resulting design, and documents the DID baseline.

Each of the elements of the LMP framework that were covered in the previous LMP documents including PRA development, LBE selection and evaluation, SSC safety classification, and selection of SSC performance and special treatment requirements are involved.

The incorporation of DID in each component of the LMP framework is illustrated in Figure 2-5 and the key elements of each box in this figure are summarized below. The color coding in this figure identifies elements of the process that are probabilistic, deterministic, and risk-informed meaning having both probabilistic and deterministic aspects. It is emphasized that the implementation of the framework is not a series of discrete tasks but rather an iterative process. The sequence of boxes reflects more an information logic than a step-by-step procedure. The execution of the DID elements is accomplished in the context of an integrated decision-making process throughout the plant design and operation lifecycle.

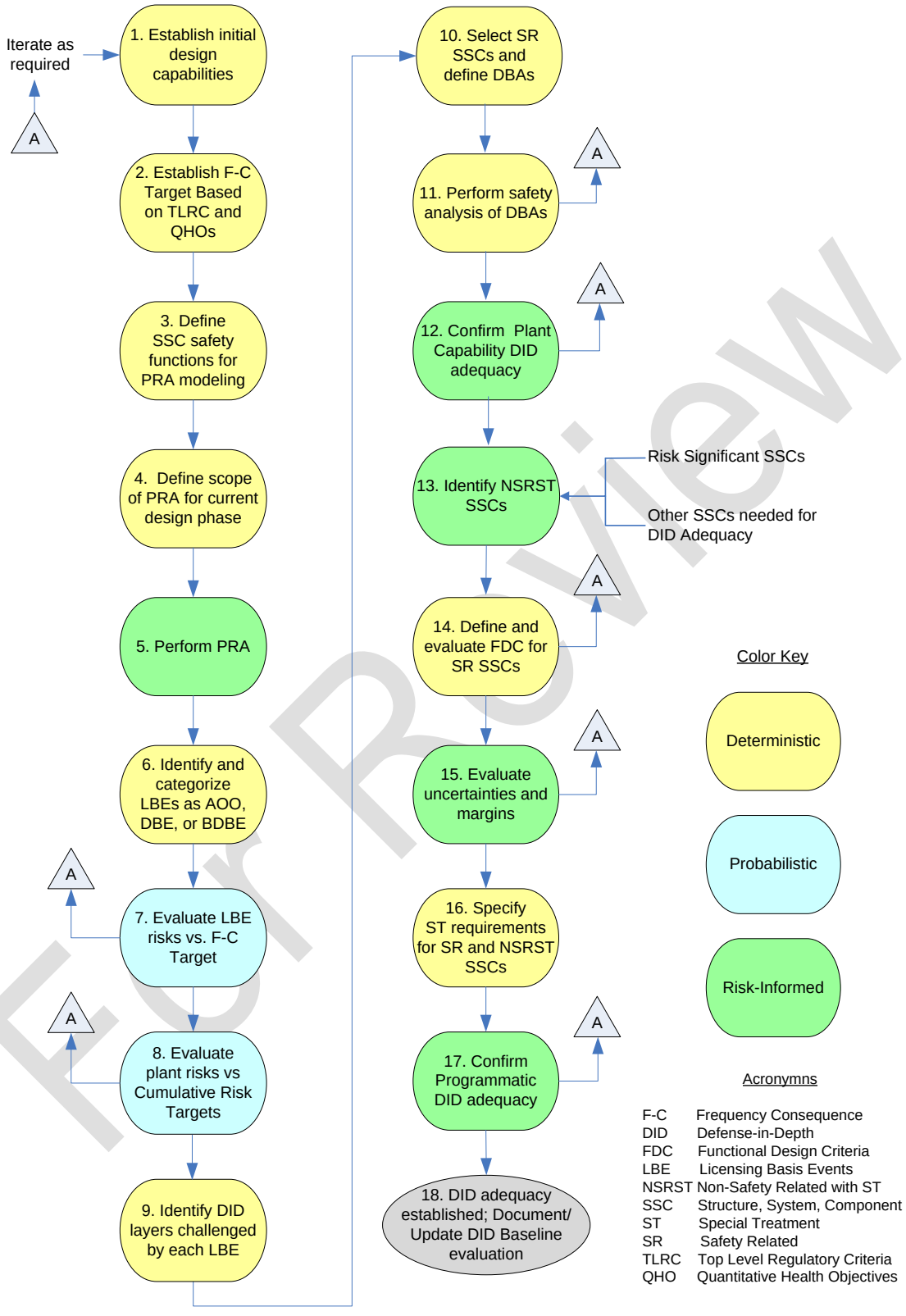


Figure 2-5. Integrated Process for Incorporation and Evaluation of Defense-in-Depth

Box 1. Establish Initial Design Capabilities

The process begins in Box 1 with available design information. Top level requirements are formulated with input from all stakeholders, including user requirements for such things as energy production, capital costs, operating and maintenance costs, safety, availability, investment protection, siting, and commercialization requirements. This framework is an integrated, iterative, and systematic top-down process. Technology development is identified to validate design assumptions and enhance confidence that user requirements will be satisfied. DID adequacy is given high priority in the early phase of design.

Even though many of these requirements are not directly associated with meeting licensing requirements, they often contribute to DID. User requirements for plant availability and reliability contribute to protecting the first layer of defense of DID in Figure 2-4 by controlling plant disturbances and preventing Initiating Events (IEs) and Anticipated Operational Occurrences (AOOs).

The selection of the inherent reactor characteristics for the design are determined by the early fundamental design decisions to address user requirements. Examples of the kinds of decisions that are made in this step include power level, selection of the materials for the reactor, moderator, and coolant, neutron energy spectrum, thermodynamic cycle, parameters of the cycle and energy balance, and evaluation of options such as fuel type, indirect versus direct cycle, passive versus active safety systems, working fluids for secondary cycles, selection of design codes for major SSCs, Operations and Maintenance (O&M) philosophy, and other high level design decisions driven by the top level requirements and results of the design trade studies. The decision whether to use inherent characteristics and passive SSCs as the primary means of assuring safety functions, supplemented by active systems that provide additional layers of defense to the prevention and mitigation of events is of particular relevance to any design.

At an early stage of design, a comprehensive set of plant level and system level functional requirements are developed. Examples of plant level requirements include requirements for passive and active fulfillment of functions, man-machine interface requirements, plant cost, plant availability, plant investment protection requirements, construction schedule, load following versus base load, barrier protections against external events, etc. This step includes the identification of systems and components and their functions, including energy production functions, maintenance functions, auxiliary functions, and safety functions and an identification of hazards associated with these SSCs. This is a purely deterministic step that produces a definition of the design in sufficient detail to begin the PRA.

The selection of inherent reactor characteristics, primary heat transport system design parameters, and materials selection for SSCs dictate the safe stable operating states for the reactor. Considerations of the need for periodic inspections and maintenance, O&M procedures, methods for starting up, shutting down, load following, and mode transitions are used to make decisions about the modes and states that need to be considered to complete the functional design and to perform the subsequent evaluations.

As part of the pre-conceptual design phase, the design process will have developed the major elements of its plant capabilities for DID as well as an initial selection of codes and standards

that form part of the programmatic DID. By addressing the fundamental top-level requirements of operability, availability, maintainability, and investment protection features for the design, using conventional practices and industry codes and standards, a great deal of the DID capability is naturally established. It is noted that additional plant capabilities as well as programs and compensating measures may be added as a result of maturing probabilistic and deterministic evaluations of DID in subsequent steps.

Initially, the designer makes decisions on both the design and selection of codes and standards that influence design and some baseline level of special treatment. For example, the designer may select certain parts of the American Society of Mechanical Engineers (ASME) design codes for certain SSCs which may be linked to ASME requirements for in-service inspection. Provisions must then be made in the design and the definition of modes and states to perform the required inspections. Final decisions on the frequency and extent of inspections will be made later in Box 14 of the figure. The full extent of special treatment is defined later following the evaluation of LBEs and the selection of SSC safety classes for each SSC. Hence, selection of codes and standards supports both the plant capabilities for DID and the activities that contribute to the programmatic DID.

As noted previously, the process of establishing DID capabilities in the plant design is an iterative process. Some portions of the design advance earlier than others, normally from the nuclear island to the power conversion and site support portions. As a result, some of the activities in Figure 2-5 are updated in parallel. Thus, the IDP process recurs more often than the serial picture as more and more of the design is completed and integrated evaluations of performance and DID become more robust.

Box 2. Establish F-C Target Based on Top Level Regulatory Criteria (TLRC) and Quantitative Health Objectives (QHOs)

The F-C target derived from TLRC is an important risk-informed element of the LMP framework as discussed more fully in the LMP LBE selection and evaluation document.[9] It plays a key role in the selection of DBAs and risk evaluation of LBEs and establishing adequate safety margins that help quantify the plant capabilities for DID. The LBE document also discusses cumulative risk targets for evaluating the total integrated risks of the multi-module plant for those non-LWRs employing a modular design. Criteria for the definition of risk significant LBEs and SSCs were developed as part of the LMP document on SSC safety classification.[11] Figure 2-6, which is taken from the document, shows the use of the F-C target to establish risk significant LBEs. As defined in this figure, risk significant LBEs have site boundary doses exceeding 2.5 mrem, which is a fraction of the background radiation exposure for 30 days, and have frequencies and consequences within 1% of the F-C target which is derived in the LMP document on LBE selection and evaluation.[9] The evaluation of DID adequacy in Boxes 12 and 17 of Figure 2-5 focuses on the LBEs and associated SSCs with the highest levels of risk significance.

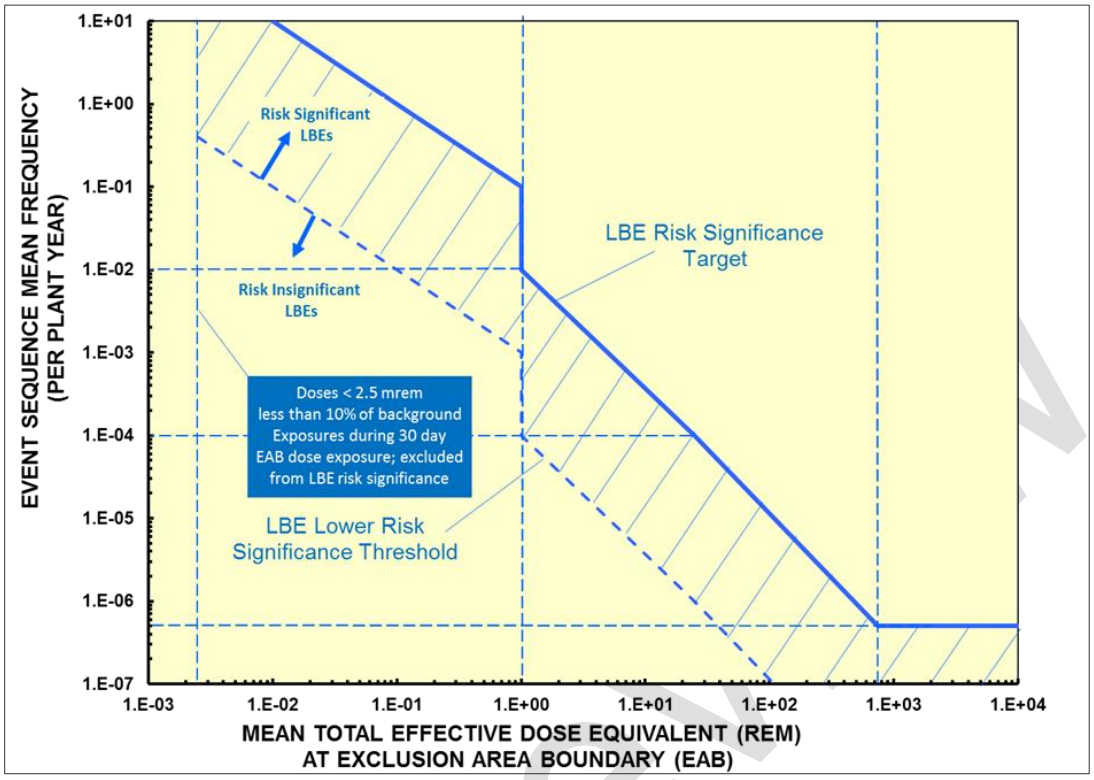


Figure 2-6. Use of F-C Target to Define Risk Significant LBEs

Box 3. Define SSC Safety Functions for PRA Modeling

The plant designer defines the reactor specific safety functions as represented in Box 3. All reactors are designed to meet certain fundamental safety functions* such as retention of radioactive material, decay heat removal, and reactivity control. However, application of the reactor specific safety design approach leads to a set of reactor specific safety functions that achieve the fundamental safety functions. During this process, the designer confirms the allocation of these safety functions to both passive and active SSCs. In Box 3, the top-level design criteria are also confirmed for all the SSCs selected to perform the reactor specific safety functions. By the time Box 3 is completed the plant capabilities that support DID are largely determined. Adjustments may be made in later steps to address the results of subsequent evaluations that may expose weaknesses in design or operating assumptions, or expose margin or other uncertainties that are relevant to demonstrate adequate levels of safety and sufficient DID.

As explained more fully in the LMP PRA document,[10] the definition of safety functions, defined as those functions responsible for the prevention and mitigation of release of radioactive material, and identification of SSCs that perform these functions is developed with close collaboration between the development of the design and the initial construction of the PRA model. These safety function definitions are essential to understand in the evaluation of the roles of SSCs in the prevention and mitigation of accidents which is a key element of DID adequacy.

*The term "fundamental safety function" is used extensively in IAEA publications such as IAEA SSR-2/1 (Rev. 1).[18] The functions listed are the ones regarded as fundamental and are applicable to all reactor technologies.

Box 4. Define Scope of PRA for Current Design Phase

In the initial stages of the design, an evaluation is made to decide which hazards, IEs, and event sequences to consider within the design basis and for designing specific measures to prevent and to mitigate off normal events and accidents.

As explained more fully in the LMP PRA document,[10] the scope and level of detail of each successive update and upgrade of the PRA is aligned to the level of detail of design and site information that is associated with each phase of the design. Depending on the stage of the design, the scope of the PRA may be extended to sources of radioactive material outside the reactor core that have their own unique safety functions, and SSCs to support those functions.

Box 5. Perform PRA

The performance of the current phase of the PRA is covered in this box consistent with the framework described in the LMP PRA document.[10] As explained more fully in the PRA document, the development and evaluation of the design and the development of the PRA model is a highly iterative process. Information from the PRA is used together with deterministic inputs to establish DID adequacy as part of the risk-informed and performance-based evaluation of DID depicted in Boxes 12 and 17. As explained more fully in the supporting LMP papers on PRA development, LBE selection and evaluation, and SSC safety classification, the PRA is used together with traditional deterministic safety approaches to affect a risk-informed process. The PRA is not employed simply to calculate numerical risk metrics, but rather to develop risk insights into the design and to identify sources of uncertainty in the PRA models and supporting data that complement the deterministic elements of the framework. The DID evaluation includes the identification of compensating protective measures to address the risk significant sources of uncertainty so identified.

Box 6. Identify and Categorize LBEs as AOOs, DBEs, or BDBEs

The process for identifying and categorizing the LBEs in terms of AOOs, DBEs, and BDBEs was discussed in detail in the LMP LBE document.[9]

Box 7. Evaluate LBE Risks vs. F-C Target

An important input to evaluating DID adequacy is to establish adequate margins between the risks of each LBE and the F-C target. Such margins also help demonstrate conformance to the NRC's advanced reactor policy objectives of achieving higher margins of safety. In this process, the most risk significant LBEs are identified. These provide a systematic means to better focus attention on those events that contribute the most to the design risk profile. This step is discussed more fully in Section 2.9 of this paper.

Box 8. Evaluate Plant Risks vs. Cumulative Risk Targets

In addition to establishing adequate margins between the risks of individual LBEs and the F-C targets, the evaluation of the margins against the cumulative risk metrics identified in the LMP LBE paper is also necessary to establish DID adequacy. This step is discussed more fully in Section 2.9 of this paper.

Box 9. Identify DID Layers Challenged by Each LBE

The layers of defense framework in Figure 2-4 are used in this box to evaluate each LBE with more attention paid to risk significant LBEs to identify and evaluate the DID attributes to support the capabilities in each layer and to minimize dependencies among the layers. An expanded discussion of this step is found in Section 2.9.

Box 10. Select Safety-Related (SR) SSCs and Define DBAs

As explained more fully in the LMP LBE[9] and SSC[11] documents, the selection of SR SSCs is accomplished by examining each of the DBEs and high consequence BDBEs and performing sensitivity analyses to determine which of the safety functions modeled in these LBEs are required to perform their prevention or mitigation functions to keep the DBEs and high consequence BDBEs inside the F-C target. Those safety functions are classified as required safety functions. In general, there may be two or more different sets of SSCs that could provide these required safety functions. Those functions specified by the design team (represented on the IDP) select which of the available SSCs that can support the required safety functions for all the DBEs and high consequence BDBEs are designated as safety-related. DBAs are then constructed starting with each DBE and then assuming only the safety-related SSCs perform their prevention or mitigation function. DID considerations are taken into account in the selection of safety-related SSCs by selecting those that yield high confidence in performing their functions with sufficient reliability and to minimize uncertainties. Examples of how DID attributes were taken into account in selecting the SR SSCs were given for the MHTGR (a specific modular high temperature gas-cooled reactor designed by General Atomics) in the LMP LBE white paper.[9]

Box 11. Perform Safety Analysis of DBAs

Conservative deterministic safety analyses of the DBAs are performed in a manner that is analogous to that for current generation light water reactors in this step of the process. The conservative assumptions used in these analyses make use of insights from the PRA which includes an analysis of the uncertainties in the plant response to events, mechanistic source terms, and radiological consequences. Programmatic DID considerations are taken into account in the formulation of the conservative assumptions for these analyses which need to show that the site boundary doses meet 10 CFR 50.34 acceptance limits.

Box 12. Confirm Plant Capability DID Adequacy

At this step of the integrated process, there is sufficient information, even during conceptual engineering phase, to evaluate the adequacy of the plant capabilities for DID using information from the previous steps and guidelines for establishing the adequacy of DID as explained in Section 2.8. This step is supported by the results of the systematic evaluation of LBEs using the layers of defense process outlined in Figure 2-4 in Box 9. As part of the DID adequacy evaluation, each LBE is evaluated to confirm that risk targets are met without exclusive reliance on a single element of design, single program, or single DID attribute. This is described more fully in Section 2.9.1.

Box 13. Identify Non-Safety-Related with Special Treatment (NSRST) SSCs

As explained more fully in the LMP SSC document, all the SSCs that participate in a layer of defense are generally not classified as SR. However, these SSCs are evaluated against criteria for establishing SSC risk significance and additional criteria for whether the SSC provides a function required for DID adequacy. Criteria for classifying SSCs as safety significant based on DID considerations is presented in Section 2.8.2 below. SSCs not classified as SR or NSRST are classified as Non-Safety-Related with No Special Treatment (NST). None of the NST SSCs are regarded as safety significant even though they may contribute to the plant capability for DID. This is true because SSCs that perform a function that prevents and/or mitigates a release of radioactive material are modeled in the PRA and are candidates for SSC classification. All of the safety significant SSCs are classified as either SR or NSRST.

Box 14. Define and Evaluate Functional Design Criteria for SR SSCs

Also explained in the LMP SSC paper is the definition of Functional Design Criteria (FDC) for SR SSCs. FDC provide a bridge between the DBAs and the formulation of principle design criteria for the SR SSCs. DID attributes such as redundancy, diversity, and independence, and the use of passive and inherent means of fulfilling safety functions are used in the formulation of FDCs.

Box 15. Evaluate Uncertainties and Margins

One of the primary motivations of employing DID attributes is to address uncertainties, including those that are reflected in the PRA estimates of frequency and consequence as well as other uncertainties which are not sufficiently characterized for uncertainty quantification nor amenable to sensitivity analyses. The plant capability DID include design margins that protect against uncertainties. The layers of defense within a design, including layer 5, off-site response, are used to compensate for residual unknowns. The approach to identifying and evaluating uncertainties that are quantified in the PRA and used to establish protective measures reflected in the plant capability and programmatic elements of DID is described in Section 2.10.

Box 16. Specify Special Treatment Requirements for SR and NSRST SSCs

According to the SSC classification approach described in the LMP SSC document,[11] all safety significant SSCs that are distributed between SR and NSRST are subject to special treatment requirements. These requirements always include specific performance requirements to provide adequate assurance that the SSCs will be capable of performing their functions with significant margins and with a high degree of reliability. These include numerical targets for SSC reliability and availability, design margins for performance of essential safety functions, and monitoring of performance against these targets with appropriate corrective actions when targets are not fully realized. Another consideration in the setting of SSC performance requirements is the need to assure that the results of the plant capability DID evaluation in Box 12 are achieved not just in the design, but in the as-built and as-operated and maintained plant following manufacturing and construction, and maintained during the life of the plant. Criteria for classifying an SSC as safety significant to meet plant capability DID adequacy are discussed in Section 2.8.2. The SSC performance targets are set by the design IDP that is responsible for establishing the adequacy of DID. In addition to these performance targets, additional special treatments may be identified as explained more fully in Section 3.5 of the LMP SSC document.[11]

Box 17. Confirm Programmatic DID Adequacy

The adequacy of the programmatic measures for DID is driven by the selection of performance requirements for the safety significant SSCs in Box 16. The programmatic measures are evaluated relative to the risk significance of the SSCs; roles of SSCs in different layers of defense and the effectiveness of special treatments in providing additional confidence that the risk significant SSCs will perform as intended.

Box 18. DID Adequacy Established; Document/Update DID Baseline Evaluation

The RIPB evaluation of DID adequacy continues until the recurring evaluation of plant and programmatic DID associated with design and PRA update cycles no longer identifies risk-significant vulnerabilities where potential compensatory actions may be needed. At this point, a DID baseline can be finalized to support the final design and operations the plant.

The successful outcomes of Boxes 12 and 17 establish DID adequacy. This determination is made by the IDP and documented initially in a DID integrated baseline evaluation report which is subsequently revised as the iterations through the design cycles and design evaluation evolve. The responsibilities of the IDP and criteria for declaring that adequate DID has been established are discussed further in Sections 2.7.2, 3.3, and 3.5.

2.6 How Major Elements of the LMP TI-RIPB Framework are Employed to Establish DID Adequacy

Another perspective on the interfaces between the LMP framework to establishing DID adequacy and the major elements of the LMP TI-RIPB framework is provided in Table 2-1. As seen in this table, there are important DID roles in each major element of the framework including:

- Designer development of the safety design approach
- Development and analysis of information from the design and design specific PRA development
- Selection and evaluation of LBEs
- Establishing the adequacy of margins in the evaluation of risk significance of LBEs, safety functions and SSCs
- SSC safety classification and development of SSC performance requirements
- Establishing the appropriate special treatment based on the insights gained from the PRA LBE development and SSC classification

Table 2-1. Role of Major Elements of LMP TI-RIPB Framework in Establishing DID Adequacy

Elements of TI-RIPB Framework	Role in Establishing DID Adequacy
Designer Development of Safety Design Approach	Selection of inherent, active, and passive design features Selection of approach to radionuclide functional and physical barriers Definition of safety functions to prevent and mitigate accidents for inclusion into the PRA Selection of passive and active SSCs to perform safety functions with consideration of the Commissions' Advanced Reactor Safety Policy to simplify designs and rely more on inherent and passive means to fulfill safety functions Initial selection of DID attributes for plant capability and programmatic DID
Reactor Specific PRA	Identification of challenges to each layer of DID and evaluation of the plant responses to them Identification of challenges to physical and functional barriers within layers of defense Characterization of the plant responses to initiating events and identification of end states involving successful mitigation and associated success criteria, and unsuccessful mitigation with release of radioactive material from one or more reactor modules or radionuclide sources Assessment of the effectiveness of barriers in retaining fission products via mechanistic source term development and assessment offsite radiological consequences Assessment of the initiating event frequencies, reliabilities, and availabilities of SSCs required to respond to those initiating events Identification of dependencies and interactions among SSCs; evaluation of the layers of defense against common cause failures and functional independence Grouping of the event sequences into LBEs based on similarity of initiating event challenge, plant response, and end state Information for the evaluation of risk significance Identification of key sources of uncertainty in modeling event sequences and estimation of frequencies and consequences Quantification of the impact of uncertainties via uncertainty and sensitivity analyses Identification and documentation of scope, assumptions, and limitations of the PRA
Selection and Evaluation of LBEs	Identification of safety margins in comparing LBE risks against F-C targets and cumulative risk criteria Evaluation of the risk significance of LBEs Confirmation of the required safety functions Input to the selection of safety-related SSCs Input to the formulation of conservative assumptions for the deterministic safety analysis of DBAs
SSC Safety Classification and Performance Requirements	Classification of NSRST and NST SSCs Selection of SSC Functional Design Criteria Selection of design requirements for safety-related SSCs Selection of performance-based reliability, availability, and capability targets for safety significant SSCs Selection of Special Treatment Requirements for safety significant SSCs
Risk-Informed Evaluation of DID Adequacy	Evaluation of DID attributes for DID Input to identification of safety significant SSCs Input to the selection of safety-related SSCs

Elements of TI-RIPB Framework	Role in Establishing DID Adequacy
	Evaluation of roles of SSCs in the prevention and mitigation of LBEs
	Evaluation of the LBEs to assure adequate functional independence of each layer of defense.
	Evaluation of single features that have a high level of risk importance to assure no overdependence on that feature and appropriate special treatment to provide greater assurance of performance
	Input to SSC performance requirements for reliability and capability of risk significant prevention and mitigation functions
	Input to SSC performance and special treatment requirements
	Integrated evaluation of the plant capability DID
	Integrated evaluation of programmatic measures for DID

The IDP uses information and insights in each of these elements to support a risk-informed and performance-based evaluation of DID adequacy. As indicated in Figure 2-3, RIPB decisions that are made in this evaluation feedback any necessary changes to the DID attributes reflected in the plant capability and programmatic elements of DID. More discussion of the IDP is found in Section 3.0.

2.7 RIPB Compensatory Action Selection and Sufficiency

2.7.1 Choosing RIPB DID Compensatory Actions

Because the design, safety analyses, and PRA will be developed in phases and in an iterative fashion, the DID adequacy evaluation and baseline are updated as the design matures. The DID evaluation can be depicted as the more detailed DID framework shown in Figure 2-3 using information as it is developed in the design process to adjust the plant capability features or programmatic actions as the state of DID knowledge improves with the design evolution.

2.7.2 Plant or Programmatic Changes

The addition of new features, improved plant capabilities, programmatic controls, or assurance activities should provide demonstrable improvements in predicted plant performance, risk reduction, elimination or material reduction of significant uncertainties, or greater assurance of plant performance. The timing of when the need for additional DID capabilities is identified should influence the decision of what form of compensatory actions are taken. Programmatic actions alone should not be taken to solve a plant performance vulnerability associated with an event that can lead directly to exceedance of an applicable safety target, goal, or regulation.

Improve Plant Capability

During the development of the functional design (pre-conceptual, conceptual, and preliminary design phases), RIPB DID insights that highlight significant adverse risks, smaller margins than desired, or overdependence on certain design features should be addressed with a bias towards improvements in the plant capability. Consideration of the practicality of potential actions should include counterproductive safety impacts such as operational complexity increases,

extended outage impacts, increased plant staff radiation exposures, and waste disposal, as well as business issues such as capital cost increases, delivery schedule impacts, and plant output and availability.

Improve Plant Performance Assurance

Programmatic actions can be important elements of safety assurance and should be used to assure that construction and operations stay within the design envelope established for the plant. The application of special treatment is in part compensation for uncertainties in performance of SSCs associated with risk significant LBEs. Other special treatments are part of effective monitoring of plant and SSC performance over time to assure the realized performance remains within the design basis.

Programmatic controls such as initial in-plant testing, risk-informed technical specifications, operating procedures for all modes and states, conservatively established alarm and control setpoints, performance monitoring programs, and corrective maintenance programs should be put in place for risk significant SSCs.

In the case where there is some uncertainty about phenomena involved in predicting plant performance, special testing should be considered, particularly early in the design process. This can take the form of actions such as additional integrated effects and separate effects testing to reduce the uncertainties in plant models (risk or safety analysis). For SSC performance variability or reliability uncertainties, they can be reduced by actions such as equipment prototype testing, equipment qualifications, manufacturing assurance or improved performance monitoring of causes of reduced equipment (or human) reliability compared to the functional reliability goals used in the RIPB design.

Reduce Residual Uncertainty

Both plant DID capabilities and programmatic DID capabilities contribute to reducing residual uncertainties. The DID evaluation of risk significant BDBEs explores the potential for rare and highly undesirable events that might occur. The choice of compensatory action includes design changes to mitigate undesirable dose consequences, reliability improvements in the physical design or the SCC special treatment applied to risk significant SSCs or a combination that provides meaningful improvements in the risk profile for the BDBE sequence. The selection of DBAs from the set of DBEs and analyzing those risk-significant events' performance with only safety-related equipment is a sensitivity study with additional conservatism built-in to the analysis to test the limits of the design. The likelihood of these DBA events is often below the threshold frequency cutoff for the risk analysis. The conservative analysis provides additional insight into the potential for other unspecified, rare events to still lead to acceptable results. Coupled with Emergency Planning programs that are capable of initiating timely public protective actions, the residual risks of unforeseen severe accidents are further minimized by the inclusion of bounding DBA evaluations.

Programmatic DID capabilities also reduce residual uncertainties through the application of actions such as independent review and oversight programs. Applications of programs such as quality assurance programs, off-site management reviews, training programs should include insights from the RIPB design products to improve their focus with a bias to risk-significant

features of the design, construction, and operations of the plant. The selection of programmatic special treatment should avoid overlapping activities as much as practical to reduce the total programmatic burden for the plant.

Life Cycle Considerations

As the design proceeds through its maturation process, the evaluation of DID adequacy should likewise mature. The early focus on DID adequacy should be on plant capability DID and should support the finalization of SSC functional requirements for risk-significant events. Early programmatic DID evaluations should focus on the adequacy and uncertainties in knowledge about plant performance that will be included in the PRA; on the translation of early risk-insights into specifications of SSC functional and reliability requirements; and, on the treatment of hazards that exist in the design that may have been screened out of the PRA. As the design matures, the DID adequacy evaluation should include the internal and external IEs included in the scope of the PRA that contribute to common cause risk-significant LBEs and ensure that the basis for screening out any hazards is technically well founded.

2.8 Establishing the Adequacy of Plant Capability DID

The RIPB evaluation of DID adequacy is complete when the recurring evaluation of plant capability and programmatic capability associated with design and PRA update cycles no longer identifies risk-significant vulnerabilities where potential compensatory actions can make a practical, significant improvement to the LBE risk profiles or risk significant reductions in the level of uncertainty in characterizing the LBE risk. The IDP is responsible for making the deliberate, affirmative decision that DID adequacy has been achieved. This decision should be clearly recorded, including the bases for this decision, in a configuration-controlled document. At this point, the DID baseline should be finalized to support the operational phase of the plant.

2.8.1 Guidelines for Plant Capability DID Adequacy

With reference to Table 2-1, the fundamental DID capability is established in the formulation of the reactor safety design approach, which is developed in a coordinated fashion with the development of the plant PRA, as discussed more fully in the LMP PRA document.[10] The plant capability DID is also influenced in the course of selecting and evaluating LBEs and in the safety classification of SSCs.

The approach to establishing plant capability DID begins in the development of the safety design approach and is accomplished in the course of the LMP iterative process steps leading up the selection and evaluation of the licensing basis events as shown in Figure 2-7 and is also impacted by the LMP framework to SSC safety classification as shown in Figure 2-8. Box 7e in Figure 2-7 represents the step in the LBE evaluation where the plant capability for DID is assessed. Information developed in the LBE selection and evaluation process is also used to support SSC safety classification which is part of plant capability DID. As discussed in the NRC documents that describe the DID philosophy, layers and DID attributes play a significant role in the approach to DID capability. However, there do not exist any well-defined regulatory acceptance criteria for deciding the sufficiency of the DID for nuclear power plant licensing or operation. To support the design and licensing of advanced non-LWRs within the LMP

framework, a set of DID adequacy guidelines has been developed. The guidelines used to evaluate the adequacy of plant capability DID proposed within the LMP framework are presented in Table 2-2.

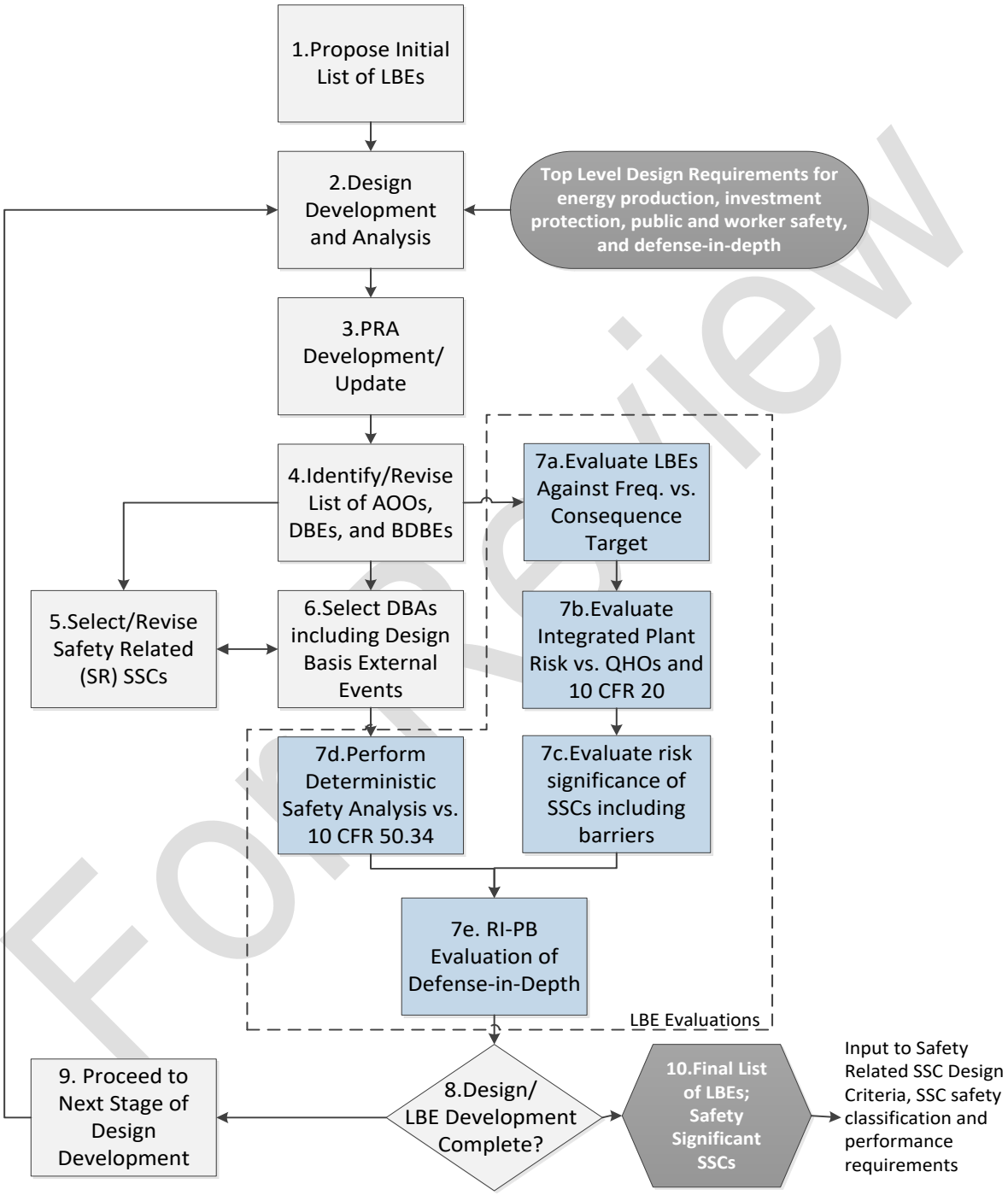


Figure 2-7. LMP Process for Selecting and Evaluating LBEs

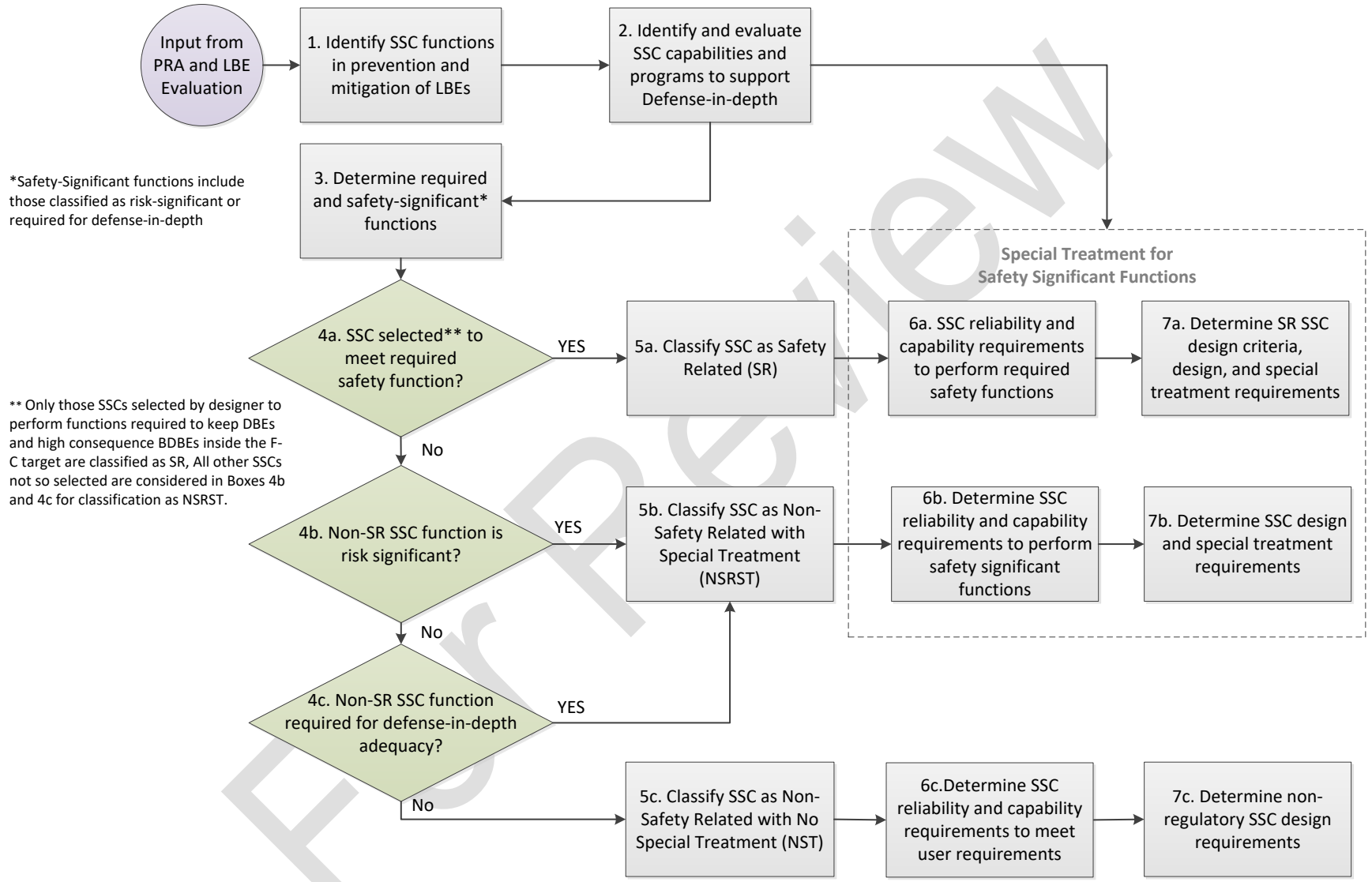


Figure 2-8. LMP Approach to the Safety Classification of SSCs and Formulation of SSC Performance Requirements

Table 2-2. 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
5) Deploy adequate offsite protective actions and prevent adverse impact on public health and safety</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>
</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.

2.8.2 DID Guidelines for Defining Safety Significant SSCs

As shown in Boxes 2 and 3 of the LMP SSC Safety Classification process in Figure 2-8, SSCs are classified as safety significant if they perform one or more functions that are classified as risk significant, or necessary for adequacy of DID. The plant capability DID adequacy guidelines in Table 2-2 require that two or more independent plant design or operational features be provided to meet the guidelines for each LBE. Any SSCs required to meet this guideline, as determined by the IDP, would be regarded as performing a safety function necessary for adequacy of plant capability DID. Such SSCs, if classified as risk significant, would already be classified as safety significant. Note that all the SR classified SSCs meet the criteria for being classified as risk significant, and hence safety significant. If one of the plant features used to meet the need for multiple DID measures in Table 2-2 involves the use of SSCs that are neither safety-related nor risk significant, the IDP would classify the SSC as safety significant and NSRST because it performs a function required for DID adequacy according to the guidelines in Table 2-2.

As explained more fully in the LMP SSC document, SSCs that are regarded as safety significant but are not SR are classified as NSRST. Special treatment requirements for NSRST SSCs include the setting of performance requirements for SSC reliability, availability, and capability and any other treatments deemed necessary by the IDP responsible for guiding the integrated design process in Figure 2-5 and evaluating the adequacy of DID. More discussion on the makeup and functions of the IDP is found in Section 3.

2.8.3 DID Attributes to Achieve Plant Capability DID Adequacy

The evaluation of plant capability DID adequacy focuses on the completeness, resiliency, and robustness of the plant design with respect to addressing all hazards, responding to identified IEs, the availability of independent levels of protection in the design for preventing and mitigating the progression of IEs, and the use of redundant and diverse means to achieve the needed levels of protection sufficient to address different threats to public health and safety. Additionally, the plant capability DID adequacy evaluation examines whether any single feature is excessively relied on to achieve public safety objectives, and if so identifies options to reduce or eliminate such dependency. The completion of the plant capability DID adequacy evaluation provides the necessary basis to conclude that there is "Adequate Protection" of public health and safety.

Table 2-3 lists the plant capability DID attributes and principal evaluation focus included in this DID evaluation scope. The evaluation of plant capability involves the systematic evaluation of hazards that exist for a given technology and specific design over the spectrum of all modes and states including anticipated transients and potential accidents within and beyond the design basis.

Table 2-3. Plant Capability Defense-In-Depth Attributes

Attribute	Evaluation Focus
Initiating Event and Accident 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 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

2.9 Evaluation of LBEs against Layers of Defense

A key element of the risk-informed, performance-based evaluation of DID is a systematic review of the LBEs against the layers of defense. This review by the IDP is necessary to evaluate the plant capabilities for DID and to identify any programmatic DID measures that may be necessary for establishing DID adequacy. This review has the following objectives:

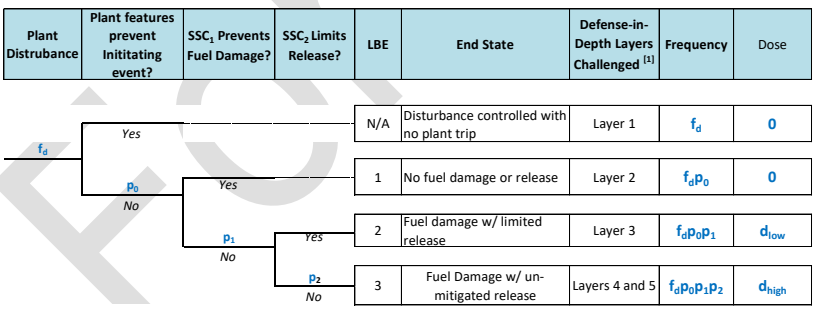
- Identify how plant capabilities for DID are deployed to prevent and mitigate each LBE at each layer of defense challenged by the LBE
- Examine the balance between accident prevention and mitigation reflected in the LBEs
- Identify the roles of SSCs that perform prevention and mitigation functions along each LBE and develop a thorough understanding in the importance of the SSC reliabilities and capabilities in contributing to plant capability DID
- Develop a deep understanding of the bases for classifying SSCs as safety-related and their capabilities to execute the required safety functions; review the technical basis for other SSCs that are classified as risk significant
- Evaluate the effectiveness of physical and functional barriers to retain radionuclides in preventing or limiting release
- Review the technical bases for important characteristics of the LBEs with focus on the most risk significant LBEs, and LBEs with relatively higher consequences.* The technical bases for relatively high frequency LBEs that are found to have little or no release or radiological consequences is also a focus of the review.

*LBEs with site boundary doses exceeding 1 rem (TEDE), the lower EPA Protective Action Guideline dose, are regarded as having relatively high consequences for this purpose.

- Identify sources of uncertainty that need to be addressed via programmatic and plant capability DID measures

As explained more fully in the LMP SSC document,[11] 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. 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 that were delineated in Figure 2-4.

This concept is illustrated in Figure 2-9, 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. An important outcome of this part of the DID evaluation is the establishment of protective measures and performance targets to achieve adequate SSC reliability and capability.



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

Figure 2-9. Evaluating SSC functions in Supporting the Layers of Defense-in-Depth

In order to understand the roles of SSCs in contributing to the plant capability DID in the context of layers of defense, it is helpful to organize the information available for each LBE from the PRA into the following generalized LBE model. An event sequence that gets grouped into an LBE can be described in terms of the following elements. This form of sequence definition lends itself to defining prevention and mitigation, and to identifying which SSCs are responsible for different degrees of prevention and mitigation.

1. An Initiating Event is an event which constitutes a challenge to the plant systems and structures responsible for control of transients and protection of the plant SSCs including the radionuclide transport barriers
2. Active SSC Response indicates the response (successes and failures) of active systems that support key safety functions responsible for protection of barriers, retention of radioactive material, and protection of the public health and safety, as defined by the accident sequence.
3. Passive SSC Response represents the response of passive design features responsible for supporting key safety functions, including the structures that form the radionuclide barriers themselves and the passive systems that protect them.
4. Barrier* Retention Factors constitute the response of each barrier to radionuclide transport from the radioactivity sources to the environment to the initiating events and safety system responses. This response is expressed as the degree of retention of radioactive material for each barrier expected for the sequence; historically, these barriers have typically included the fuel elements, the coolant pressure boundary, and the reactor building barrier. Depending on the reactor design, the reactor building barrier may be described as a leak tight or vented containment, confinement, reactor building or containment system barrier. For some technologies such as pool-type liquid metal reactors which lack a coolant pressure boundary, or homogeneous fuel/coolant reactors, which lack a barrier between the fuel and the coolant, the definition of barriers must be formulated appropriately in a modified version of Equation (1) below. For such technologies, the concept of barriers must be generalized to denote each item in the radionuclide transport pathway that is responsible for retention or reduction of the quantity of radionuclides that are released from the source to the environment.
5. Emergency Plan Response indicates the implementation of emergency plan protective actions to mitigate the radiological consequences to the public of a given release from the plant.

A generalized model for describing an event sequence in terms of the design features that support prevention and mitigation reflecting the above insights is provided in Table 2-4. This

*In this paper, the term "barrier" is used to denote any plant feature that is responsible to either full or partial reduction of the quantity of radionuclide material that may be released during an LBE. It includes features such as physical or functional barriers or any feature that is responsible as part of a layer of defense for mitigating the quantity of material released from the plant including time delays during fission product transport that permit radionuclide decay or provide extended response times for alternative compensatory actions.

table provides an important feedback mechanism between risk-informed and performance-based evaluation of DID and plant capability DID. The event sequence framework is part of the risk-informed evaluation of DID, and the roles of SSCs in the prevention and mitigation of accidents are the result of the plant capability DID. The reliabilities and capabilities of the SSCs that prevent and mitigate events are influenced by both the plant capability and programmatic DID elements. Programmatic DID reduces the uncertainty in the reliability and capability performance of the SSCs responsible for prevention and mitigation.

Table 2-4. Event Sequence Model Framework for Evaluating Plant Capabilities for Prevention and Mitigation of LBEs

Standard Elements of Accident Sequence	Design Features Contributing to Prevention	Design Features Contributing to Mitigation
Initiating Event Occurrence	Reliability of SSCs supporting power generation reduces the IE frequencies; successful operation of the SSCs prevents the sequence.	Capabilities of normally operating systems to continue operating during disturbances to prevent initiating events serve to mitigate events and faults that may challenge these functions.
Response of Active SSCs Supporting Safety Functions: Successful and Failed SSCs	Reliability and availability of active SSCs reduce sequence frequency; successful operation of these SSCs prevents the sequence.	Capabilities of active successful SSCs including design margins reduce the impacts of the initiating events and reduce the challenges to barrier integrity.
Response of Passive Features Supporting Safety Functions: Successful and Failed SSCs	Reliability and availability of passive SSCs reduce sequence frequency; successful operation of these SSCs prevents the sequence.	Capabilities of passive successful SSCs including design margins reduce the impacts of the initiating events and reduce the challenges to barrier integrity.
Fraction of Source Term Released from Fuel	None	Inherent and passive capabilities of the fuel including design margins given successful active or passive SSCs limit the release from the fuel.
Fraction of Source Term Released from the Coolant Pressure Boundary	None	Inherent and passive capabilities of the pressure boundary including design margins given successful active or passive SSCs and the capabilities of the fuel limit the release from the pressure boundary.
Fraction of Source Term Released from Reactor Building Barrier	None	Inherent and passive capabilities of the reactor building barrier including design margins conditioned on the successful response of any active or passive SSCs along the sequence and the capabilities of the fuel and coolant pressure boundary limit the release from the reactor building barrier.
Time to Implement Emergency Plan Protective Actions	None	Inherent and passive features and capabilities of the fuel, coolant pressure boundary, and reactor building barrier including design margins conditioned on the successful response of any active or passive SSC along the sequence dictate the time available for emergency response.

The accident sequence framework for evaluating accident prevention and mitigation in Table 2-4 is used to define a simple model for estimating the risk of a release of radionuclides associated with a specific accident sequence, or LBE:

$$R_j = Q * F_{IE,j} * P_{ASSC,j} * P_{PSSC,j} * r_{fuel,j} * r_{PB,j} * r_{cont,j} \quad (1)$$

R_j = Expected quantity of radioactive material released per year from sequence j

Q = Quantity of radionuclides (for a given isotope) in the reactor core inventory

$F_{IE,j}$ = Frequency of the initiating event associated with sequence j

$P_{ASSC,j}$ = Probability of active SSCs successes and failures along sequence j

$P_{PSSC,j}$ = Probability of passive SSCs successes and failures along sequence j

$r_{fuel,j}$ = Release fraction from the fuel barrier, given system and structure response for sequence j

$r_{PB,j}$ = Release fraction from the coolant pressure boundary for sequence j

$r_{cont,j}$ = Release fraction from the reactor building barrier for sequence j

To demonstrate the application of this concept, an LBE evaluation example has been performed of selected event sequences from the MHTGR PRA taken from Reference [2]. This example evaluation is performed for the following three selected LBEs:

1. MHTGR-1: Moderate size leak in the Helium Pressure Boundary (HPB) of less than 13 in^2; successful reactor trip and continued operation of one of the forced convection cooling systems; releases limited to circulating activity and some lift-off of plated out radionuclides. This sequence is a representative Design Basis Event for the MHTGR.
2. MHTGR-2: Small leak in the HPB of less than 1 in^2; successful reactor trip, failure of the active forced convection cooling systems; conduction cool down of the core using the active Reactor Cavity Cooling System (RCCS); releases limited to circulating activity and delayed release from small fraction of initially failed fuel particles that is minimized due to the successful HPB pump down along this sequence. This sequence is also a Design Basis Event but with a lower frequency and higher potential for release than MHTGR-1.
3. MHTGR-3: Small leak in the HPB of less than 1 in^2; successful reactor trip; failure of the active forced convection cooling systems; failure of the active RCCS; conduction cool-down to the passive reactor cavity heat sinks; releases limited to circulating activity and delayed release from small fraction of initially failed fuel particles (somewhat larger fraction than in Sequence 2). This sequence is representative of a Beyond Design Basis Event for the MHTGR.

The LBE risk plot in Figure 2-10 shows the frequencies and consequences of these three event sequences in which the consequences are expressed in terms of curie releases of the nuclide I-131, which has been shown to be a highly risk significant radionuclide for event sequences for high temperature gas-cooled reactors. By tracing through the terms of Equation (1) for these sequences the roles of SSCs responsible for accident prevention and mitigation can be easily identified using the logic of Figure 2-9. By comparing the risks of these sequences to the certainty of the radionuclide inventory, the risk reduction factors for each prevention and mitigation element can be identified.

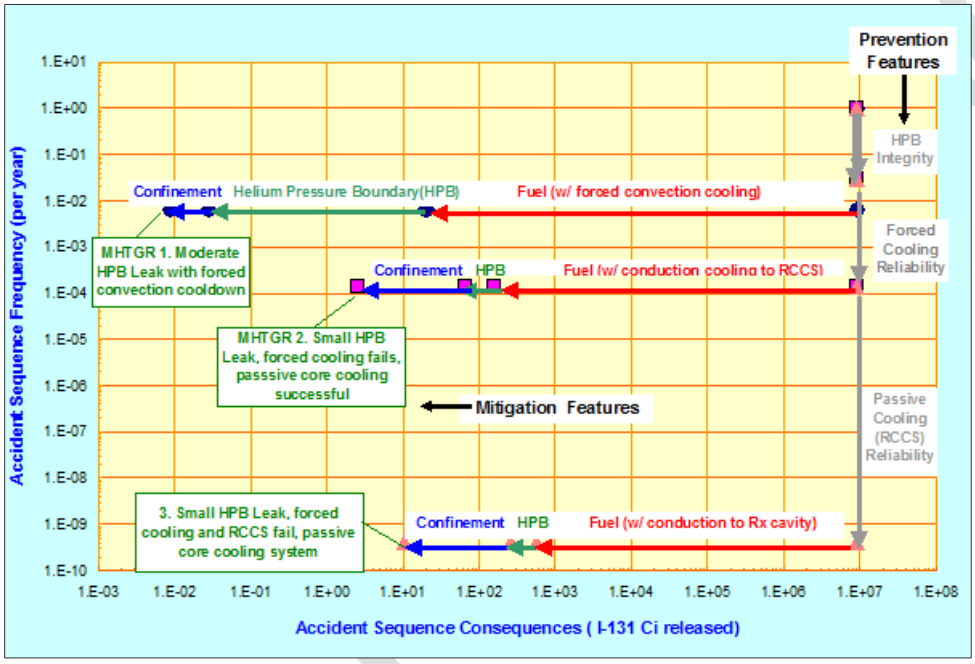


Figure 2-10. Example Evaluation of SSCs Responsible for Preventing and Mitigating MHTGR LBEs[2]

As seen in the figures, the roles of prevention and mitigation for MHTGR-1 include tow orders of magnitude of prevention by the reliability of the HPB, and nine orders of magnitude of mitigation by the radionuclide barriers. For this sequence, there is a low level of importance of the reactor building barrier due to the roles of the fuel and HPB in retaining the vast proportion of the inventory.

MHTGR-2 involves a small breach in the HPB followed by failure of the active SSCs supporting core cooling functions. The mitigation level for this sequence is aided by a passive core cooling capability that prevents significant releases from the fuel, although the releases are somewhat higher than in Sequence MHTGR-1. In MHTGR-3 there is failure of both active and passive core cooling systems following the pressure boundary breach, but the passive capability of the reactor to retain its fuel inventory is still significant as the core is still cooled by conduction and radiation to the reactor building heat sinks. An important insight about the prevention and mitigation analysis for these MTHGR sequences is that the mitigation importance of the fuel retention is significant for each of the selected. The roles of the barriers and the SSCs supporting each barrier are seen to be significantly different for each of the selected LBEs

Using this approach in the LMP framework, all the risk significant LBEs as well as the LBEs used to select the DBAs and to identify the risk significant SSCs will be examined by the IDP to help evaluate the adequacy of the plant capability DID and to determine the need for programmatic measures.

2.9.1 Evaluation of LBE and Plant Risk Margins

The purpose of this section is to explain how margins are established between the frequencies and consequences of individual LBEs and the F-C target used to evaluate the risk significance of LBEs. These margins are established for the LBEs having the highest risk significance within each of the three LBE categories (AOOs, DBEs, and BDBEs). The example margins discussed below are developed using the MHTGR LBE results.[12] The MHTGR events selected for this margin analysis include AOO-5 (small helium pressure boundary leak), DBE-10 (large helium pressure boundary leak), and BDBE-2 (moisture in leakage with delayed steam generator isolation).

Margins are developed in two forms. In Table 2-5, the margins to the F-C target are measured based on mean values of the LBE frequencies and doses as illustrated in Figure 2-11. In each case, margin is expressed as a ratio of the event's mean value (frequency and dose) to the corresponding F-C target value (frequency and dose). These are the best measure of the margins because traditionally in the PRA community, mean values are compared to targets such as design objectives for core damage frequency and large early release frequency and the NRC safety goal QHOs. Note that DBE-10 in the MHTGR was classified as a DBE because the frequency criteria for classifying DBEs in the MHTGR was 10^{-4} per plant year to 0.025 per plant year.

Table 2-5. Risk Margins based on Mean Values of LBE Frequency and Dose

LBE Category	Limiting LBE[a]			F-C Target			
	Name	Mean Freq. /plant-yr.	Mean Dose (Rem)	Freq. at LBE Dose/plant-yr. [b]	Mean Frequency Margin[c]	Dose at LBE Freq. (Rem) [d]	Dose Margin[e]
AOO	AOO-5	4.00E-02	2.50E-04	4.00E+02	1.00E+04	1.00E+00	4.00E+03
DBE	DBE-10	1.00E-02	2.00E-03	6.00E+01	6.00E+03	1.00E+00	5.00E+02
BDBE	BDBE-2	3.00E-06	4.00E-03	2.50E+01	8.30E+06	2.50E+02	6.00E+04

Notes:
[a] The Limiting LBE is the LBE with the highest risk significance in the LBE category
[b] Frequency value measured at the LBE mean Dose level from the F-C target, See [2] in Figure 2-11
[c] Ratio of the frequency in note [b] to the LBE mean frequency, mean frequency margin
[d] Dose value measured at the LBE mean frequency from the F-C target, See [4] in Figure 2-11
[e] Ratio of the Dose in Note [d] to the LBE mean dose, Mean Dose Margin

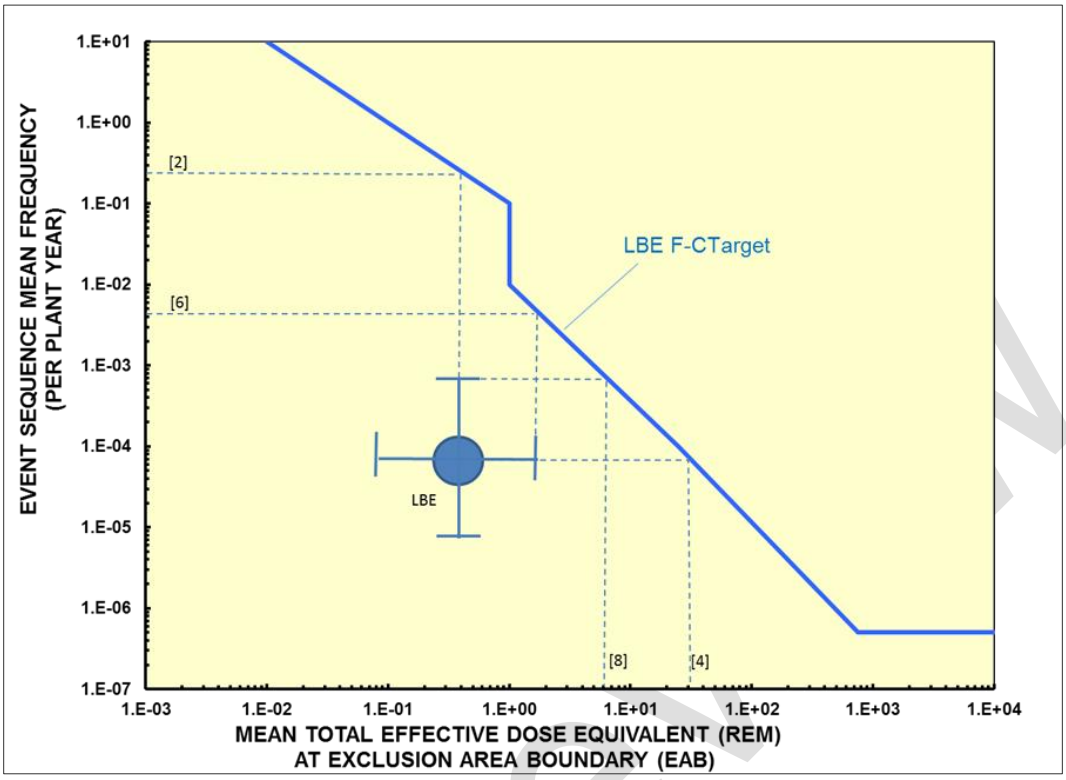


Figure 2-11. Guidance for Defining Margins Between LBE Frequencies and Doses Relative to the F-C Target

A more conservative evaluation of margins is supported in Table 2-6 in which the 95th percentile upper bound values for both LBE frequency and dose are used to calculate the margins.

Table 2-6. Risk Margins Based on 95th Percentile Values of LBE Frequency and Dose

LBE Category	Limiting LBE[a]			F-C Target			
	LBE Name	95th Percentile Freq./plant-yr.	95th Percentile Dose (Rem)	Freq. at LBE Dose/plant-yr.[b]	95th Percentile Frequency Margin[c]	Dose at LBE Freq.(Rem)[d]	95th Percentile Dose Margin[e]
AOO	AOO-5	8.00E-02	1.10E-03	9.00E+01	1.13E+03	1.00E+00	9.09E+02
DBE	DBE-10	2.00E-02	6.00E-03	2.00E+01	1.00E+03	1.00E+00	1.67E+02
BDBE	BDBE-2	1.00E-05	1.50E-02	8.00E+00	8.00E+05	1.00E+02	6.67E+03

Notes:
[a] Limiting LBE is LBE with highest risk significance in LBE Category
[b] Frequency value measured at the LBE 95th percentile Dose level from the F-C target, See [6] in Figure 2-11
[c] Ratio of the frequency in note [2] to the LBE 95th percentile frequency, 95th percentile Frequency Margin
[d] Dose value measured at the LBE 95th percentile frequency from the F-C target, See [8] in Figure 2-11
[e] Ratio of the Dose in note [d] to the LBE 95th percentile dose, 95th percentile Dose Margin

As seen in these tables for the MHTGR, the mean frequency margins range from about 6,000 to more than 8 million, and the mean dose margins range from 500 to 6,000 when the mean values

are used. When the margins are based on the 95th percentile frequencies and doses, the frequency margins range from 1,000 to 800,000 and the dose margins range from 167 to more than 6,000. Guidance for calculating the margins is provided by the table footnotes which refer to key points in Figure 2-11. This process is repeated for each individual LBE, grouped by LBE category as part of the DID evaluation during the design development.

2.9.2 Integrated Decision Panel Focus in LBE Review

The evaluation of LBEs by the IDP will focus on the following questions:

- Is the selection of initiating events and event sequences reflected in the LBEs sufficiently complete? Are the uncertainties in the estimation of LBE frequency, plant response to events, mechanistic source terms, and dose well characterized? Are there sources of uncertainty not adequately addressed?
- Have all risk significant LBEs and SSCs been identified?
- Has the PRA evaluation provided an adequate assessment of "cliff edge effects?"
- Is the technical basis for identifying the required safety functions adequate?
- Is the selection of the SR SSCs to perform the require safety functions appropriate?
- Have protective measures to manage the risks of multi-module and multi-radiological source accidents been adequately defined?
- Have protective measures to manage the risks of all risk significant LBEs been identified, especially those with relatively high consequences?
- Have protective measures to manage the risks for all risk significant common cause initiating events such as support system faults, internal plant hazards such as fires and floods, and external hazards been identified?
- Is the risk benefit of all assigned protective measures well characterized, e.g., via sensitivity analyses?

If the evaluation identifies unacceptable answers to any of these questions, additional compensatory action would be considered, depending on the risk significance of the LBE. With reference to Figure 2-5, which identifies feedback loops in the overall LMP framework at each evaluation step of the process, the compensatory action can take on different forms including changes to design and operation, refinements to the PRA, revisions to the selection of LBEs and safety classification of SSCs, as well as enhancements to the programmatic elements of DID.

2.10 Establishing the Adequacy of Programmatic DID

2.10.1 Guidelines for Programmatic DID Adequacy

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 Table 2-7.

Table 2-7. 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

The attributes of programmatic DID complement each other and provide overlapping assurance that the design plant capability is achieved in design, manufacturing, construction, and operations lifecycle phases. The evaluation focus items in Table 2-7 should be answered for each programmatic DID attribute for risk significant LBEs in order to determine that the programmatic DID provides sufficient confidence that there is reasonable assurance of adequate protection of public health and safety based on the design plant capability. The net result establishing and evaluating programmatic DID is the selection of special treatment programs for all safety significant SSCs, which include those classified as SR or NSRST.

2.10.2 Application of Programmatic DID Guidelines

In the evaluation of programmatic DID using the attributes in Table 2-7 and the questions raised in Table 2-8, the considerations discussed below will be used by the IDP.

Table 2-8. 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 risk-informed DBA 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?
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?

Attribute	Evaluation Focus	Implementation Strategies	Evaluation Considerations
	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?

Quality and Reliability

The initial quality of the design is developed through the application of proven practices and application of industry codes and standards. In cases where no approved codes and standards are available, conservative adaptation of existing practices from other industries or first principles derivations of repeatable practices may be required. Conservatism should be applied in cases were common practices and codes are not available. The use of new practices should be validated to the degree practical against physical tests or other operating experiences if risk significant SSCs are involved. The PRA should consider the uncertainties of unproven methods or standards for specific risk significant functions. This question should be examined by the IDP.

The execution of work for risk-significant portions of the design should be consistent with risk importance of the plant functions and associated SSCs. As discussed more fully in the LMP paper on SSC safety classification, Graded Quality Assurance should be applied NSRST SSCs based on the layer of defense and for risk significant SSC safety functions.

The primary focus on reliability in the evaluation of DID is on the establishment of the functional reliability targets for SSCs that prevent or mitigate risk significant LBEs as part of a layer of defense and associated monitoring of reliability performance against the targets. The reliability can be achieved by some combination of inherent, passive, or active SSC capabilities. The appropriate use of redundancy and diversity to achieve the reliability targets set by the IDP together with the plant technical specifications should be evaluated.

Margin Adequacy

At the plant level, performance margins to established design goals and regulatory limits are evaluated as part of DID adequacy. At the individual SSC level, properly designing SSCs to proven codes and standards provides an appropriate level of design margin in the level of assurance that the SSC will perform reliably at its design conditions and normally include reserve margin for more demanding conditions. The DID evaluation should include a determination that the appropriate codes were applied to safety significant SSCs (included in SR and NSRST safety categories) and that the most demanding normal operation, AOO, DBE, or DBA parameters for that component, conservatively estimated, have been used for the design point. For SSCs that play a role in risk-significant BDBEs, the DID evaluation should evaluate the inherent performance margins in SSCs against the potentially more severe conditions of BDBEs in the PRA.

Treatment of Uncertainty in Programmatic DID

In judging DID adequacy, at each stage of design and operations, designers, managers, owners, and operations staff must continually keep in mind that errors are possible, equipment can fail and real events do not always mimic analytical events. For that reason, the "risk triplet" questions: "What can go wrong?" "How likely is it?" "What are the consequences?" must become an institutionalized set of questions as a part of deciding the how to deal with residual risk and uncertainty. The primary means to address these residual risks is through effective Severe Accident Management Programs and effective Emergency Planning. Siting and Emergency Planning Zone size considerations take into account the known risks of a plant, siting

in less populated areas, and having proactive Emergency Planning programs that take precautionary actions well before a serious threat to public health can arise.

Compensation for Unknowns

The layers of defense approach utilized in the proposed DID evaluation framework includes the need to define protective measures to address unknowns. Feedback from actual operating and maintenance experience to the PRA provides performance-based outcomes that are part of plant monitoring. Periodic PRA updates should incorporate that information into reliability (system or human) estimates to determine whether significant LBE risks have changed or new events emerged. All nuclear industry sources of information should be utilized for known, risk-significant LBEs.

Operator and management training programs should contain appropriate requirements for dealing with each identified risk significant BDBEs, and include provision for event management of potential accidents undefined in the PRA due to truncation or other limitations in modeling or scope for this phase of the design/PRA development. The evaluation of programmatic DID should determine whether risk-significant LBEs are included in the routine training of operators and management.

Programmatic DID in Design

Programmatic activities developed during design and licensing phases that are integral to design process include design-sensitive programs such as:

- Graded quality programs for SSC design, manufacturing, construction, and testing
- Development of risk-informed plant technical specifications
- Tier 1 and inspections, tests, analyses, and acceptance criteria
- Operating procedures including those for DBEs, DBAs and BDBEs
- Maintenance programs for safety significant SSCs (SR and NSRST))
- In-service inspection and in-service testing programs

The early consideration of the use of RIPB practices to establish the scope of these types of programmatic actions supports the more efficient implementation of physical design features that minimize the scope of compliance activities and related burdens in the operational phase of the plant lifecycle.

Examples of special treatment programs are listed in Table 2-9. The actual special treatments are established by the IDP, as discussed more fully in Section 3.0. Each of these programs and treatments are programmatic DID protective measures that should benefit from RIPB insights early in their development cycles in optimizing their value as part of an integrated risk management approach. Using a risk-informed approach to grade the activities based on the predicted performance of all risk significant LBEs provides a systematic application of programmatic activities that provide reasonable assurance of adequate protection of the public.

Table 2-9. Examples of Special Treatments Considered for Programmatic DID

Programs	Elements
Engineering Assurance Programs	Special treatment specifications Independent design reviews Physical testing and validation including integrated and separate effects tests
Organizational and Human Factors Programs	Plant simulation and human factors engineering Training and qualification of personnel Emergency operating procedures Accident management guidelines
Technical Specifications	Limiting conditions for operation Surveillance testing requirements Allowable outage (completion) times
Plant Construction and Start-Up Programs	Equipment fabrication oversight Construction oversight Factory testing and qualification Start-up testing
Maintenance and Monitoring of SSC Performance Programs	Operation In-service testing In-service inspection Maintenance of SSCs Monitoring of performance against reliability and capability performance indicators
Quality Assurance Program	Inspections and audits Procurement Independent reviews Software verification and validation
Corrective Action Programs	Event trending Cause analysis Closure effectiveness
Independent Oversight and Monitoring Programs	
Equipment Qualification	Seismic qualification Adverse environment qualification Physical protection
Emergency Planning	

There are other programmatic activities spread across a broader portion of the industry that provide additional levels of programmatic DID and contribute to reasonable assurance of adequate protection of the public. The NRC, Institute of Nuclear Power Operations, American Nuclear Insurers, ASME, and IAEA all play an important part of assuring public safety through their independent oversight and monitoring of the different phases of plant development and operations. Included in some of these oversight activities are self-reporting requirements that

notify NRC and other external agencies of unexpected or inappropriate performance of SSCs or human activities.

3.0 RISK-INFORMED AND PERFORMANCE-BASED EVALUATION OF DID ADEQUACY

3.1 Purpose and Scope of Integrated Decision Panel Activities

Under the LMP framework, an IDP will be responsible for evaluating the adequacy of DID. 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,[13] such panels are employed to guide the risk-informed decision-making process. The Nuclear Energy Institute (NEI) has developed procedures and guidelines for the makeup and responsibilities of such panels.[14][15] Specifically, NEI 00-04 Sections 9 and 11 provide valuable guidance on the composition of a panel (referred to as the Integrated Decision-making Panel within NEI 00-04) and the associated output documentation. The decisions of the IDP should be documented and retained as a quality record; this function is critical to future decision making regarding plant changes which have the potential to affect DID.

For advanced non-LWRs that are currently in various stages of design development, the IDP is comprised of a team that is responsible for implementing the integrated process steps for evaluating DID shown in Figure 2-5. This team includes those responsible for the design, operations, and maintenance program development and for performing the necessary deterministic and probabilistic evaluations identified in this figure.

3.2 Risk-Informed and Performance-Based Decision Process

The IDP will use a risk-informed and performance-based integrated decision-making (RIPB-DM) process. Risk-informed decision-making is the structured, repeatable process by which decisions are made on significant nuclear safety matters including consideration of deterministic and probabilistic inputs. The process is also performance-based because it employs measurable and quantifiable performance metrics to guide the decision that DID is adequate. RIPB-DM plays a key role in designing and evaluating the DID layers of defense and establishing measures associated with each plant capability and programmatic DID attribute described in Section 2.

Table 3-1 provides a listing of the integrated decision-making attributes and principal evaluation focus included in the RIPB DID evaluation scope to be executed by the IDP. The RIDM process is expected to be applied at each phase of the design processes in conjunction with other integrated review processes executed during design development as described in Figure 2-5. Meeting the applicable portions of ASME/ANS PRA Standard for Advanced non-LWRs,[16] which includes the requirement for and completion of the appropriate PRA peer review process, is required for use of the PRA in RIPB-DM processes.

Table 3-1. 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 Modeling 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

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

A key concept in DID adequacy evaluation RIPB-DM is that a graded approach to RIPB-DM is prudently applied such that the decisions on LBEs with the greatest potential risk significance receive corresponding escalated cross-functional and managerial attention, while routine decisions are made at lower levels of the organization consistent with their design control program.

Completing the evaluation of the DID adequacy of a design is not a one-time activity. The Designer is expected to employ the RIPB-DM process as often as required to minimize the potential for revisions late in the design process due to DID considerations. Integrated DID adequacy evaluations would be expected to occur in concert with completion of each major phase of design—conceptual, preliminary, detailed, and final—and would additionally occur in response to any significant design changes or new risk significant information at any phase of design or licensing.

3.3 IDP Actions to Establish DID Adequacy

Adequacy of DID is confirmed when the following actions and decisions by the IDP are completed.

- Plant capability DID is deemed to be adequate.
  - Plant capability DID guidelines in Table 2-2 are satisfied.
  - Review of LBEs is completed with satisfactory results.
    - Risk margins against F-C target are sufficient.
    - Risk margins against Cumulative Risk Targets are met.
    - Role of SSCs in the prevention and mitigation at each layer of defense challenged by each LBE is understood.
    - Prevention/mitigation balance is sufficient.
    - Classification of SSCs into SR, NSRST, and NST is appropriate.
    - Risk significance classification of LBEs and SSCs are appropriate.
    - Independence among design features at each layer of defense is sufficient.
    - Design margins in plant capabilities are adequate to address uncertainties identified in the PRA.
- Programmatic DID is deemed to be adequate.
  - Performance targets for SSC reliability and capability are established.
  - Source of uncertainty in selection and evaluation of LBE risks are identified.
    - Completeness in selection of initiating events and event sequences is sufficient.
    - Uncertainties in the estimation of LBE frequencies are evaluated.
    - Uncertainties in the plant response to events are evaluated.
    - Uncertainties in the estimation of mechanistic source terms are evaluated.
    - Design margins in plant capabilities are adequate to address residual uncertainties.
  - Special treatment for all SR and NSRST SSCs is sufficient.

3.4 IDP Considerations in the Evaluation of DID Adequacy

Risk Triplet Examination

The evaluation of DID adequacy requires recurring examination of the design as it matures. Thus, there needs to a recurring consideration of the three basic questions in the risk triplet: "What can go wrong?", "How likely is it?", and "What are the consequences?" This should be done at the natural design phase review points as specific engineering information is "baselined"

for the next design phase. In the reviews, hazards analysis updates, PRA updates, DBA safety analysis and plant level risk profiles (e.g. LBEs identified, changes in margins or uncertainties, or layers of defense features, human performance assumptions, etc.) should be an explicit component of the review and decision to continue to the next engineering phase.

State of Knowledge

The level of knowledge during a design process matures from functional capabilities at plant and system level to physical characteristics that implement the functional design. During the period of early design evolution, trade studies that explore alternative configurations, alternate materials, inherent, passive and active system capabilities, etc. to most effectively achieve top level project criteria should be considered in light of DID objectives. Different PRA and non-PRA tools, commensurate with the availability of design information, should be utilized to provide risk insights to the designer as an integral part of the design development process. The scope and level of detail of the PRA will evolve as the level of design and site information matures. Relative risk and reliability analyses should be developed in advance of the full PRA as they provide very valuable inputs to design functionality requirements as well early means to resolve operational challenges. It is during this period of the design development, basic decisions on layers of defense that comprise a portion of the DID strategy are best formulated and documented and evaluated in appropriate design descriptions at plant and system level.

Margin Adequacy

Once the initial PRA is developed, LBEs are available for examination. The margins between mean performance predictions and any insights into uncertainties around that performance should be evaluated as part of establishing an early DID baseline. Other sources of uncertainty caused by PRA scope boundaries, model incompleteness, methods or input data accuracy should be examined as well. The focus and level of scrutiny between no/low consequence LBEs and higher consequence LBEs should vary according to the risk significance.

Sources of Uncertainties

The greatest number of uncertainties exist in the beginning of the design cycle and systematically are resolved through the iterative design process. Those are state-of-knowledge uncertainties that are transient in nature, they are unverified assumptions that are worked out over the design process and sometimes beyond. During design phase reviews, the DID evaluation should examine significant assumptions or features that could materially alter plant or individual LBE risk profiles or whether there are single features that are risk significant that would benefit from additional compensatory actions to improve performance capability or performance assurance.

Permanent uncertainties are typically broken down into two groups, those that are caused by variability or randomness, such as plant performance, and those that are as a result of gaps in knowledge. DID adequacy evaluations should include both types of permanent uncertainties in reaching a final design adequacy conclusion. Attention in the evaluation of DID adequacy is paid to hazards excluded from the PRA that could either pose an on-site risk to plant or personnel performance; and, those that could be a risk to the public due to significant non-radiological consequences.

Magnitude of Uncertainties

DID adequacy evaluations will examine the nominal performance of the plant against various risk objectives. Evaluations will also include quantified uncertainties for PRA-derived LBE's in two ways, frequency uncertainty and consequence uncertainty. These are described more fully in the PRA and LBE guidelines.

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.

3.5 Baseline Evaluation of Defense-in-Depth

As illustrated in Figure 2-5, there will be a number of iterations through the integrated design process to reflect different design development phases and the feedback loops indicated in Figure 2-3 where the DID evaluation leads to changes in the plant design to enhance the plant capability DID or changes to the protective measures reflected in the programmatic DID. 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 first complete pass through the integrated design process will require a baseline DID evaluation which completes the actions of the IDP summarized in the previous section. The baseline DID evaluation will be documented in sufficient detail so it can be efficiently updated in future design development iterations. The checklists in Table 3-2 and Table 3-3 will serve as a reminder as to the scope of the evaluation which will be documented in a controlled document.

Table 3-2. Evaluation Summary – Qualitative Evaluation of Plant Capability DID

LBE IE Series Name	Functional			Physical	
	Margin Adequacy	Multiple Protective Measures	Prevention and Mitigation Balance	Functional Reliability	No Single Feature Relied Upon
Normal Operation	√			√	
AOOs	√			√	
DBEs	√	√	√	√	√
BDBEs	√	√	√	√	√
DBAs	√	√	√	√	√

Table 3-3. Evaluation Summary – Qualitative Evaluation of Programmatic DID

LBE IE Series Name	Quality/Reliability: Design, Manufacturing, Construction, O&M	Compensation for Uncertainties			Offsite Response: Emergency Response Capability
		Human Errors	Mechanical Failures	Unknowns	
Normal Operation	√	√	√	√	
AOOs	√	√	√	√	
DBEs	√	√	√	√	√
BDBEs	√	√	√	√	√
DBAs	√	√	√	√	√

3.6 Considerations in Documenting Evaluation of Plant Capability and Programmatic DID

Simplify Change Evaluation

The documentation of the DID baseline shall be derived from the design records, primarily those that verified the attributes described in Section 2 were adequate. The threshold for evaluating a change to the DID baseline should be informed by the risk significance of changes in LBE performance in the PRA. This involves the following considerations as part of the RIDM process for plant changes:

- Does the change introduce a new LBE for the plant?
- Does the change increase the risk of LBEs previously considered to be of no/low risk significance to the point that it will be considered risk-significant after the change is made?
- Does the change reduce number of layers of defense for any impacted LBEs or materially alter the effectiveness of an existing layer of defense?
- Does the change significantly increase the dependency on a single feature relied on in risk-significant LBEs?

If the answer to any of the above questions is yes, a complete evaluation of all of the DID attributes as described in Section 2 is performed. As a result of the more comprehensive evaluation of DID changes, the IDP will reject the change or recommend additional compensatory actions to plant capability or programmatic capability if practical to return a baseline LBE performance to within the current DID baseline. If the compensatory actions are

not effective, the change may require NRC notification in accordance with current license and regulatory requirements.

The evaluation of DID adequacy should be documented in two parts; quantitative and qualitative, covering the DID attributes established above. The summary the DID baseline includes.

Quantification of LBE Margins Against F-C Target

The purpose is to explain how margins are established between the frequencies and consequences of individual LBEs and the F-C target used to evaluate the risk significance of LBEs. These margins are established for the LBEs having the highest risk significance within each of the three LBE categories: AOOs, DBEs, and BDBEs. This was described more completely in Section 2.9.1.

Summary Evaluation of DID Adequacy Baseline

Additionally, qualitative evaluation of DID adequacy is performed for each LBE. Adequate qualitative DID is provided when a qualitative evaluation determines observable attributes of the design demonstrate the conservative principles supporting DID are, in combination, sufficient. The conclusion is reached through an integrated decision-making process to verify the following are in place commensurate with the identified event risks.

3.7 Evaluation of Changes to Defense-in-Depth

For each iteration of the design evaluation life cycle in Figure 2-5, the DID evaluation from the baseline will be re-evaluated based on a review to determine which programmatic or plant capability attributes have been affected for each layer of defense. Obviously changes that impact the definition and evaluation of LBEs, safety classification of SSCs, or risk significance of LBEs or SSCs will need to have the DID adequacy re-evaluated and the baseline updated as appropriate.

4.0 REFERENCES

[1] Idaho National Laboratory, "Next Generation Nuclear Plant Defense-in-Depth Approach," INL/EXT 09-17139, December 2009 [ADAMS Accession No. ML093480191].

[2] PBMR Pty. Ltd., "Defense-in-Depth Approach for the Pebble Bed Modular Reactor," Document Number 043593, November 2006.

[3] American Nuclear Society, ANSI/ANS-53.1-2011, "Nuclear Safety Design Process for Modular Helium-Cooled Reactor Plants," December 21, 2011.

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

[5] U.S. Nuclear Regulatory Commission, NUREG/KM-0009, "Historical Review and Observations of Defense-in-Depth," April 2016.

[6] U.S. Nuclear Regulatory Commission, DG-1285, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis," March 2017.

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

[8] SECY 1998-0144, "White Paper on Risk-Informed and Performance-Based Regulation (Revised)," June 22, 1998, and Staff Requirements Memorandum dated March 1, 1999.

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

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

[11] 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.

[12] U.S. Department of Energy, "Preliminary Safety Information Document for the Standard MHTGR," DOE-HTGR-86-024, September 1988.

[13] 10 CFR 50.69, "Risk-Informed Categorization and Treatment of Structures, Systems and Components for Nuclear Power Reactors," December 2, 2015.

[14] Nuclear Energy Institute, NEI-00-04, 10 CFR 50.69, "SSC Categorization Guideline," July 2005.

[15] Nuclear Energy Institute, RIEP-NEI-16, 10 CFR 50.69, "Risk Informed Engineering Programs," Revision 0, November 2016.

[16] American Society of Mechanical Engineers and American Nuclear Society, "Probabilistic Risk Assessment Standard for Advanced non-LWR Nuclear Power Plants," RA-S-1.4-2013.

[17] 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.

[18] International Atomic Energy Agency, "Safety of Nuclear Power Plants: Design Specific Safety Requirements," No. SSR-2/1 (Rev. 1), 2016.

Reckley, William

From: AUSTGEN, Kati <kra@nei.org>
Sent: Tuesday, December 12, 2017 10:31 AM
To: Reckley, William; Cubbage, Amy
Cc: Amir Afzali (aafzali@southernco.com); TSCHILTZ, Michael; ZACHARIAH, Thomas; Ed Wallace (ed.wallace@gnbcassociates.com); Karl Fleming (karlfleming@comcast.net); Peter S Hastings (peter@hastings-group.com)
Subject: [External_Sender] Draft LMP Defense-in-Depth White Paper
Attachments: LMP DID Draft.pdf

Bill and Amy,

Please find attached a draft of the Licensing Modernization Project's (LMP's) "Risk-Informed and Performance-Based Evaluation of Defense-in-Depth Adequacy" white paper for NRC staff review. As we have discussed, NRC observations on this paper will be used to craft associated content in the upcoming risk-informed, performance-based guidance document for advanced non-light water reactor development.

LMP efforts are led by Southern Nuclear, sponsored in part by the US Department of Energy, under the auspices of NEI's Advanced Reactor Regulatory Task Force (ARRTF). This draft has undergone review by various industry representatives (i.e., NEI's ARRTF and Idaho National Laboratory staff). We look forward to NRC staff feedback.

Please provide any comments to NEI and Southern Nuclear via the contacts copied on this email.

Thank you,

Kati Austgen | *Sr. Project Manager, New Plant, SMR & Advanced Reactors*
1201 F Street, NW, Suite 1100 | Washington, DC 20004
P: 202.739.8068 M: 202.340.1224
nei.org