INL/EXT-20-57941-Revision-0

Modernization of Technical Requirements for Licensing of Advanced Non-Light Water Reactors: Risk-Informed and Performance-Based Evaluation of Defense-in-Depth Adequacy

Wayne L Moe, Amir Afzali

Changing the World's Energy Future

Idaho National Laboratory

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

INL/EXT-20-57941-Revision-0

Modernization of Technical Requirements for Licensing of Advanced Non-Light Water Reactors: Risk-Informed and Performance-Based Evaluation of Defense-in-Depth Adequacy

Wayne L Moe, Amir Afzali

March 2020

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

Southern Company

Modernization of Technical Requirements for Licensing of Advanced Non-Light Water Reactors: Risk-Informed and Performance-Based Evaluation of Defense-in-Depth Adequacy

Document Number
SC-29980-103 Rev 1

March 2020

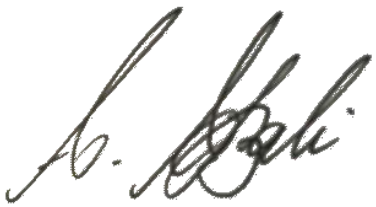
Prepared for:
U.S. Department of Energy (DOE)
Office of Nuclear Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

Southern Company

Modernization of Technical Requirements for Licensing of Advanced Non-Light Water Reactors: Risk-Informed and Performance-Based Evaluation of Defense-in-Depth Adequacy

Document Number
SC-29980-103 Rev 1

Issued by:



3/23/2020

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

Date

Disclaimer

Abstract

This document supports the work contained in Nuclear Energy Institute (NEI) 18-04 "Risk-Informed Performance-Based Technology Inclusive Guidance for Advanced Reactor Licensing Basis Development" Revision 0.[19] NEI 18-04 presents a modern, technology-inclusive, risk-informed, and performance-based (TI-RIPB) process for selection of Licensing Basis Events (LBEs); safety classification of structures, systems, and components (SSCs) and associated risk-informed special treatments; and determination of defense-in-depth (DID) adequacy for non-LWRs. The NEI guidance document provides one acceptable means for addressing the aforementioned topics as part of demonstrating a specific design provides reasonable assurance of adequate radiological protection.

This report provides the framework and associated methodology guidelines and discussion 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 led by Southern Company and cost-shared by the United States Department of Energy and has benefited from considerable NRC formal reviews[20][21] and public workshops.

The methodology converts the DID philosophy into a structured process that is implementable, embraces existing United States and international definitions and philosophies of DID that set the foundation for the process. It builds on the DID framework developed in the Department of Energy Next Generation Nuclear Plant Project and earlier works on this subject.

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. 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 report 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 methodology 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 methodology 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 methodology is then used for formulating DID strategies that can be implemented as part of the plant capability and programmatic DID elements covering the design, manufacturing, construction, testing, and operational activities that support reasonable assurance of adequate protection determinations of public radiological safety. When implemented, the Licensing Modernization Project DID methodology 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
DBEHL	Design Basis External Hazard Level
DID	defense-in-depth
DOE	Department of Energy
EAB	Exclusion Area Boundary
ES	Event Sequence
F-C	Frequency-Consequence
F-C Target	Frequency-Consequence Target
FSF*	Fundamental Safety Function
HPB	Helium Pressure Boundary
IAEA	International Atomic Energy Agency
IDP	Integrated Decision-Making Process
IDPP	Integrated Decision-Making Process 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
MST	Mechanistic Source Term
NEI	Nuclear Energy Institute
NGNP	Next Generation Nuclear Plant
non-LWR	non-light water reactor
NRC	Nuclear Regulatory Commission
NSRST	Non-Safety-Related with Special Treatment
NST	Non-Safety-Related with No Special Treatment
O&M	Operations and Maintenance
PB	performance-based
PIRT	Phenomena Identification and Ranking Table
POS	Plant Operating State
PRA	probabilistic risk assessment
PSF*	PRA Safety Function
QA	quality assurance
QHO	Quantitative Health Objective
RCCS	Reactor Cavity Cooling System
rem	Roentgen equivalent man
RFDC	Required Functional Design Criteria
RI	risk-informed
RIDM	risk-informed integrated decision-making
RIPB	risk-informed and performance-based
RIPB-DM	risk-informed and performance-based integrated decision-making
RSF*	Required Safety Function
SR	Safety-Related
SRDC	Safety-Related Design Criteria
SSCs	structures, systems, and components
TEDE	Total Effective Dose Equivalent
TI-RIPB	technology-inclusive, risk-informed, and performance-based
TLST	Top Level Safety Target
U.S.	United States

*These terms have special meanings defined in this paper. See the Glossary.

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 United States Nuclear Regulatory Commission (NRC), a formal definition that permits an objective assessment of DID adequacy has not been realized. This process provides 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 as an integral part of the overall design process. DID should be 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 DID framework in this paper embraces the definitions of the DID philosophy provided by international regulatory authorities including the NRC and International Atomic Energy Agency (IAEA). The LMP methodology 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 ANSI/ANS-53.1-2011[3] to define a technology-inclusive methodology 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 risk-informed and performance-based (RIPB) decisions regarding design; plant risk assessment; selection and evaluation of Licensing Basis Events (LBEs); 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 report is to describe the LMP framework and methodology 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 methodology is based on the premise that DID is an integral part of the design that 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 methodology described in this report 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 RIPB 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 report are to:

- Establish alignment with accepted descriptions 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 document, 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 lifecycle
- 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 Reports

The DID evaluation methodology described in this report is intended to be used in conjunction with other aspects of the LMP methodology described in the supporting reports outlined below.

The LMP team prepared independent reports on each of the four major LMP elements. Additionally, the LMP team produced a narrative report describing the processes, events, and documents involved in producing the ultimate project deliverable product, NEI 18-04 "Risk-Informed Performance-Based Technology Inclusive Guidance for Non-Light Water Reactor Licensing Basis Development." Finally, the LMP team produced a report based on the experiences of early adopters of the LMP RIPB process which includes best practices, lessons learned, and frequently asked questions and responses. See Table 1-1 for the Southern Company document numbers of each of these reports.

Table 1-1. LMP Reports and Document Numbers

Report Title	*Southern Company Document Number*	*DOE OSTI Document Number*
Selection and Evaluation of Licensing Basis Events	SC-29980-100 Rev 1	TBD
Probabilistic Risk Assessment Approach	SC-29980-101 Rev 1	TBD
Safety Classification and Performance Criteria for Structures, Systems, and Components	SC-29980-102 Rev 1	TBD
Risk-Informed and Performance-Based Evaluation of Defense-in-Depth Adequacy	SC-29980-103 Rev 1	TBD
Final Project Report	SC-29980-105 Rev. 1	TBD
LMP Lessons Learned, Best Practices, and Frequently Asked Questions	SC-29980-106 Rev 0	TBD

Probabilistic Rick Assessment (PRA) Approach

The LMP PRA Approach report[10] 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 -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 are addressed to achieve DID adequacy. The current report discusses how uncertainties exposed by the PRA are evaluated in the DID process to identify protective strategies for compensating for uncertainties.

Selection and Evaluation of LBEs

Inputs to the selection of LBEs are derived from a PRA of an advanced non-LWR plant. These inputs together with deterministic inputs, such as design selections and selection of Safety-Related (SR) 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 report,[9] the engineering and safety analysis effort will result in a selection of a set of SR SSCs that are necessary and sufficient to perform the PRA Safety Functions (PSFs) 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 SR 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 report describes how LBEs are reviewed to identify the layers of defense in the design, evaluate margins against risk targets, evaluate uncertainties in the risk evaluation, and set performance targets for plant reliability and capability which comprise important elements of programmatic DID.

Safety Classification and Performance Criteria for SSCs

The SSC report[11] describes the LMP approach for the safety classification of SSCs, selection of Required Functional Design Criteria (RFDC) for SR SSCs, and selection of performance requirements for SSC reliability and capability, with special treatment for safety significant SSCs. The SSC report covers how DID attributes are reflected in the selection of these performance requirements and the monitoring of performance against these requirements.

LMP Final Report

The LMP team produced a narrative report describing the processes, events, and documents involved in producing the ultimate Project deliverable product, NEI 18-04 “Risk-Informed Performance-Based Technology Inclusive Guidance for Non-Light Water Reactor Licensing Basis Development”. This report contains a wealth of references to documents that future users of the LMP RIPB process may find useful. Tables within the report provide references to the NRC Agencywide Document Management System (ADAMS) Accession Numbers of many industry and NRC documents that future permit and license applicants may wish to reference in their own applications.

LMP Lessons Learned, Best Practices, and Frequently Asked Questions and Responses

The LMP team produced a report based on the experiences of early adopters of the LMP RIPB process which includes best practices, lessons learned, and frequently asked questions with responses. This report provides guidance to reactor designers on how to efficiently implement the LMP RIPB processes within their own organization and answers to thirty-two frequently asked questions from reactor designers.

2.0 LMP FRAMEWORK FOR ESTABLISHING ADEQUACY OF DID

2.1 General Objectives for DID Evaluation Process

Consistent with LMP reports 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 those current regulatory requirements applicable to non-LWR technologies. 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 DID Philosophy

According to the NRC glossary,[4] DID 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 illustrates 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 2005 IAEA Safety Report Series No. 46, "Assessment of Defense in Depth for Nuclear Power Plants."[7]

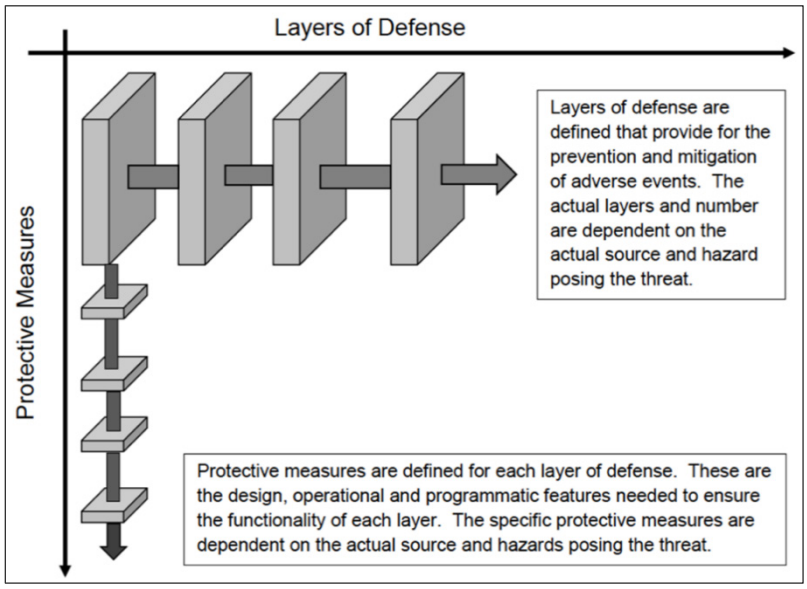


Figure 2-1. United States NRC's DID Concept[5]

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

2.3 NGNP DID Framework

The LMP framework for establishing DID adequacy builds on the DID framework that was incorporated into the American Nuclear Society design standard for modular helium-cooled reactors[3] and was developed for the NGNP project. Although this early framework was

developed for use with high-temperature gas-cooled reactors, it was envisioned as a reactor-technology neutral approach. Figure 2-2 illustrates the NGNP DID framework. The three major elements of the process are described below.

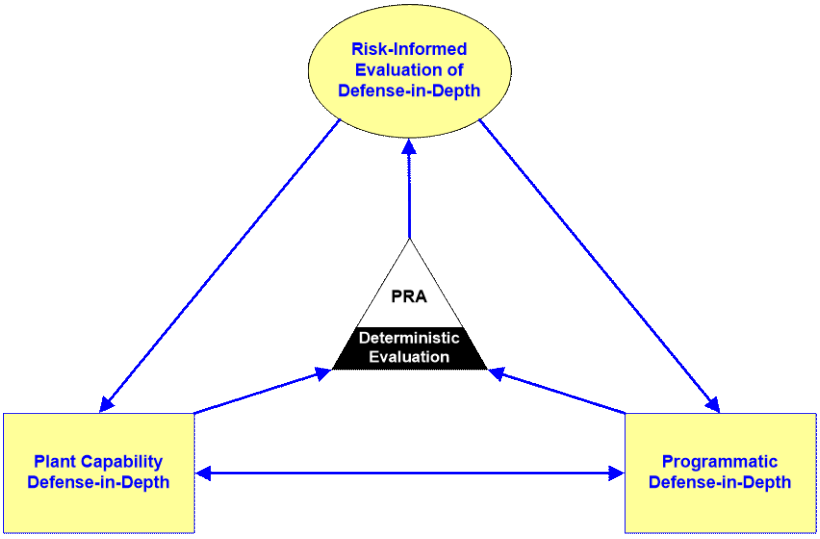


Figure 2-2. NGNP DID Framework[1]

Plant Capability DID

This element is used by the designer to select functions, SSCs, and their bounding design capabilities to assure safety adequacy. Additionally, excess capability, reflected in the design margins of individual SSCs 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 LBEs 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 DID

Programmatic DID is used to address uncertainties when evaluating plant capability DID and is used 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 DID

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 process (IDP) to assess sufficiency of DID and to enable consideration of different alternatives for achieving commensurate safety levels at reduced burdens. The outcome of the RI decision making 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 expanded to show components of each element of the methodology outlined in Figure 2-3.

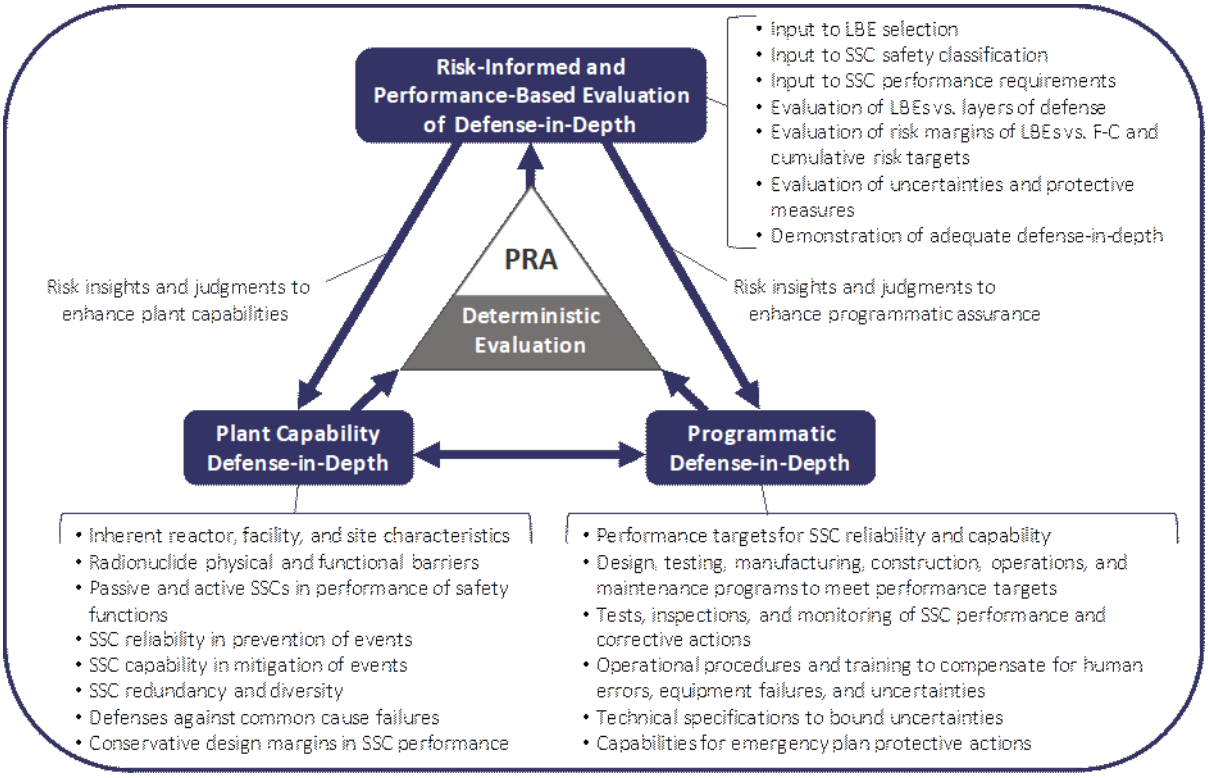


Figure 2-3. LMP Framework for Establishing DID Adequacy

*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 and evaluation and SSC safety classification 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 report.

The concept of 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 framework sets the context to evaluate each LBE and to identify the DID attributes that have been incorporated into the design to prevent and mitigate accident sequences and 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.

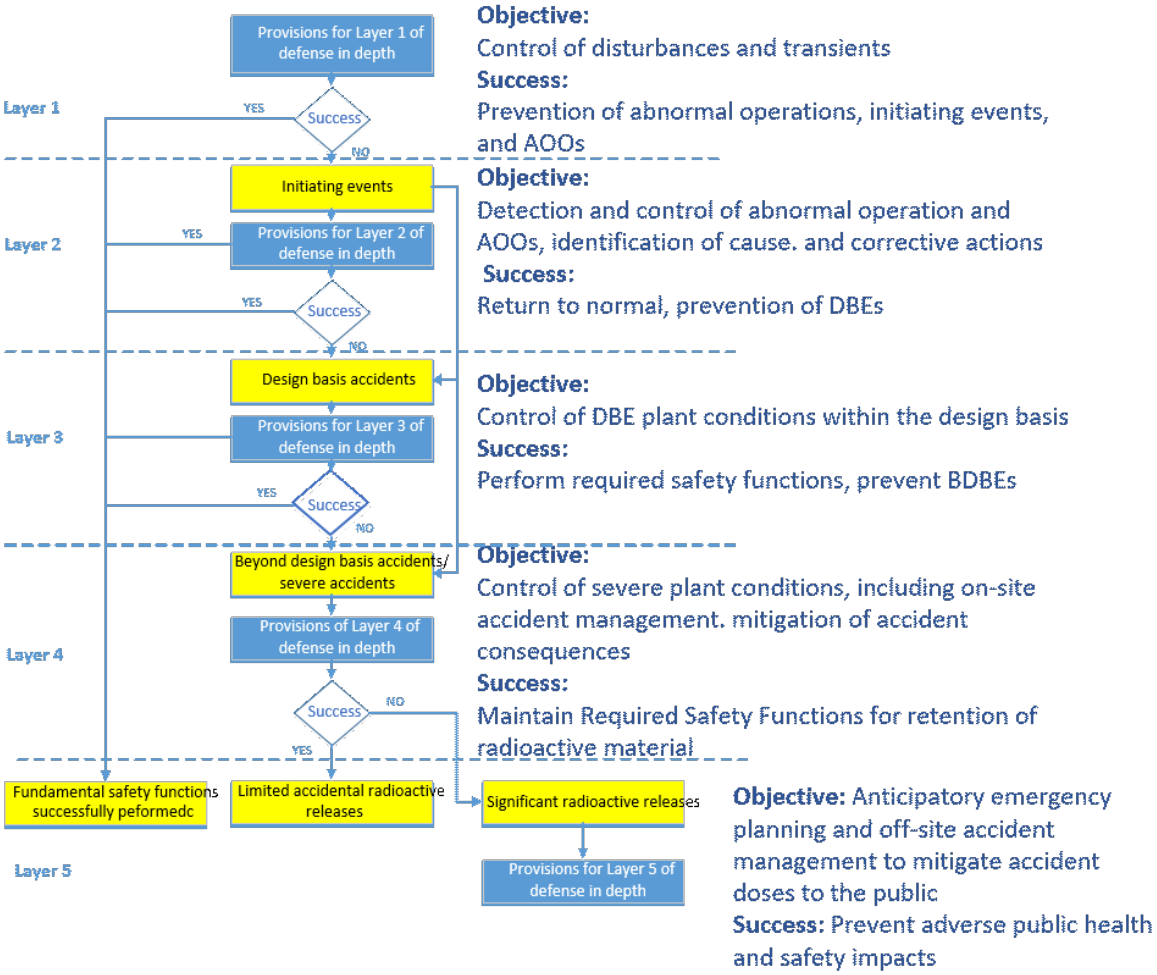


Figure 2-4. LMP Process for Evaluating LBEs Using Layers-of-Defense Concept Adapted from IAEA[7]

As explained more fully in the sections 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 in both the frequency and consequence estimates.

2.5 LMP Integrated Framework for Incorporation and Evaluation of DID

DID is considered and 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 public 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 use of an IDP within their design control process that 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.

Figure 2-5 illustrates the incorporation of DID in each component of the LMP methodology, and the key elements of each task in this figure are summarized below. Note that Figure 2-3 includes many actions described previously by the LMP methodology as a whole and does not imply that these tasks need to be re-performed for the purpose of the DID adequacy evaluation. Rather the DID adequacy evaluation considers the prior work when coming to an integrated decision on DID adequacy. The color coding in Figure 2-5 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 tasks reflects more an information logic than a step-by-step procedure. As shown by the Triangle A icons in the figure, this iteration is expected to occur repeatedly and at different tasks in the overall process. Iteration through the tasks is expected to continue through the documentation of the DID baseline in Task 18, and then with subsequent DID baseline updates as the design progresses. The execution of the DID elements is accomplished in the context of an IDP throughout the plant design and operation lifecycle.

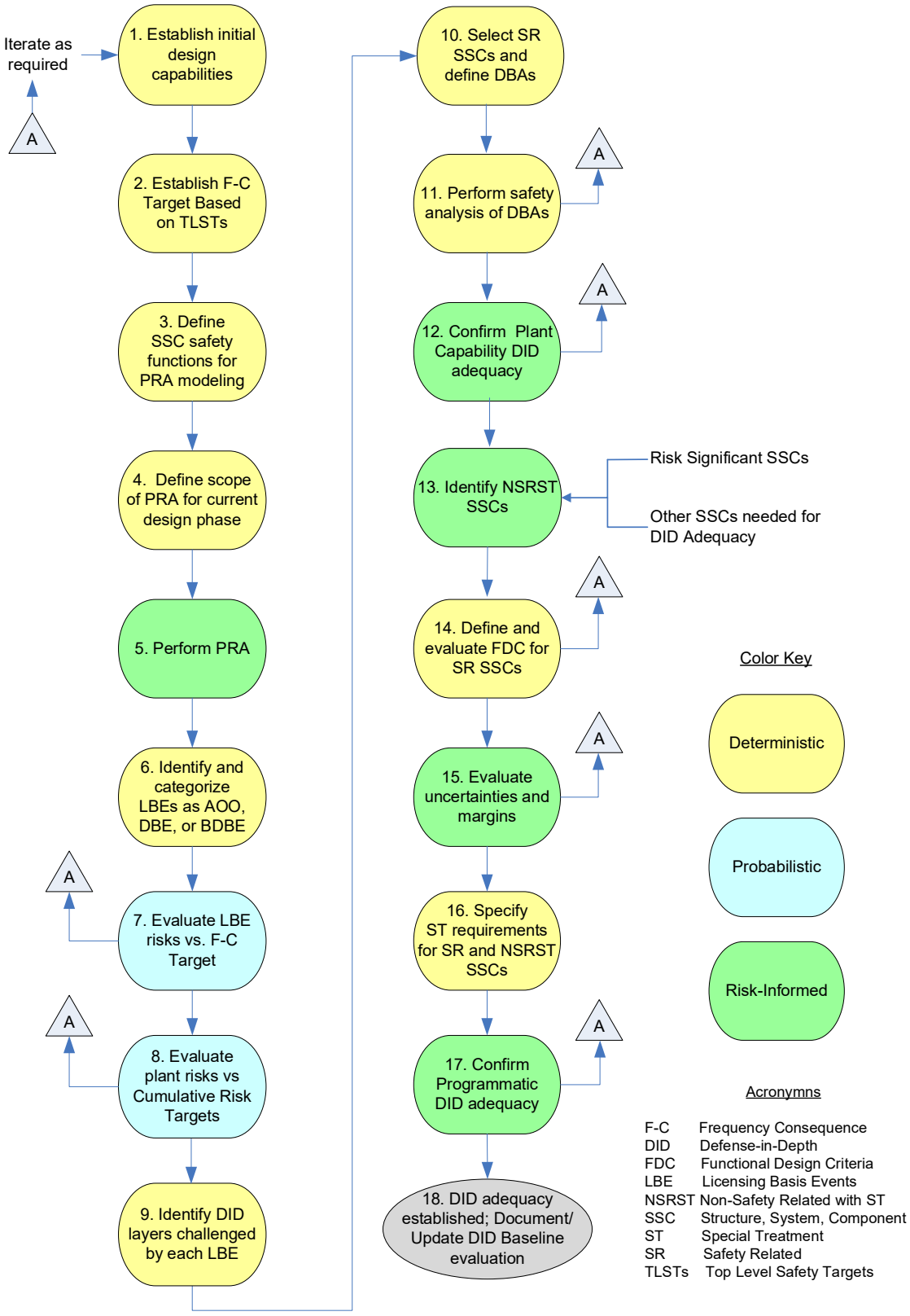


Figure 2-5. Integrated Process for Incorporation and Evaluation of DID

Task 1. Establish Initial Design Capabilities

The process begins in Task 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. 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 some Initiating Events (IEs) and AOOs.

The selection of the inherent reactor characteristics for the design are determined by the early fundamental design decisions to address user requirements, operating experience, studies of technology maturity, system engineering requirements, and safety objectives. Examples of the kinds of decisions that are made in this task 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; 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 PSFs,[*] 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 task 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, and 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.

[*]The representation of SSC safety functions in the LBEs is based on the safety functions modeled in the PRA, which are defined as those functions responsible for prevention or mitigation of the release of radioactive material from any radionuclide source within the scope of the PRA. These are referred to as PRA Safety Functions (PSFs).

As part of the pre-conceptual design phase, a great deal of the DID capability is naturally established by addressing the fundamental top-level requirements of any design for operability, availability, maintainability, and investment protection features for the design, using conventional practices and industry codes and standards, etc. 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 plant safety and DID in subsequent tasks.

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 that 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 Task 14. 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, 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 recurs more often than the serial picture as more as more of the design is completed and integrated evaluations of performance and DID become more robust.

Task 2. Establish F-C Target Derived from Top-Level Safety Targets (TLSTs)

The F-C Target derived from TLSTs is an important risk-informed element of the LMP framework as discussed more fully in the LMP LBE selection and evaluation report. It plays a key role in the evaluation of risk-significance of LBEs and in the identification of the PSFs that are necessary and sufficient to keep the DBEs at an acceptable level of risk. In the LMP methodology these are referred to as Required Safety Functions (RSFs). RSFs play a key role in the selection of safety related SSCs and definition of DBAs. Margins between the frequencies and consequences of the LBEs and the F-C Target are used to help evaluate the plant capabilities for DID. The LBE report 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 SSCs were developed as part of the LMP report on SSC safety classification. Figure 2-6, which is taken from the report, 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 that is derived in the LMP report on LBE selection and evaluation. The evaluation of DID adequacy in Tasks 12 and 17 of Figure 2-5 focuses on the LBEs and associated SSCs with the highest levels of risk significance.

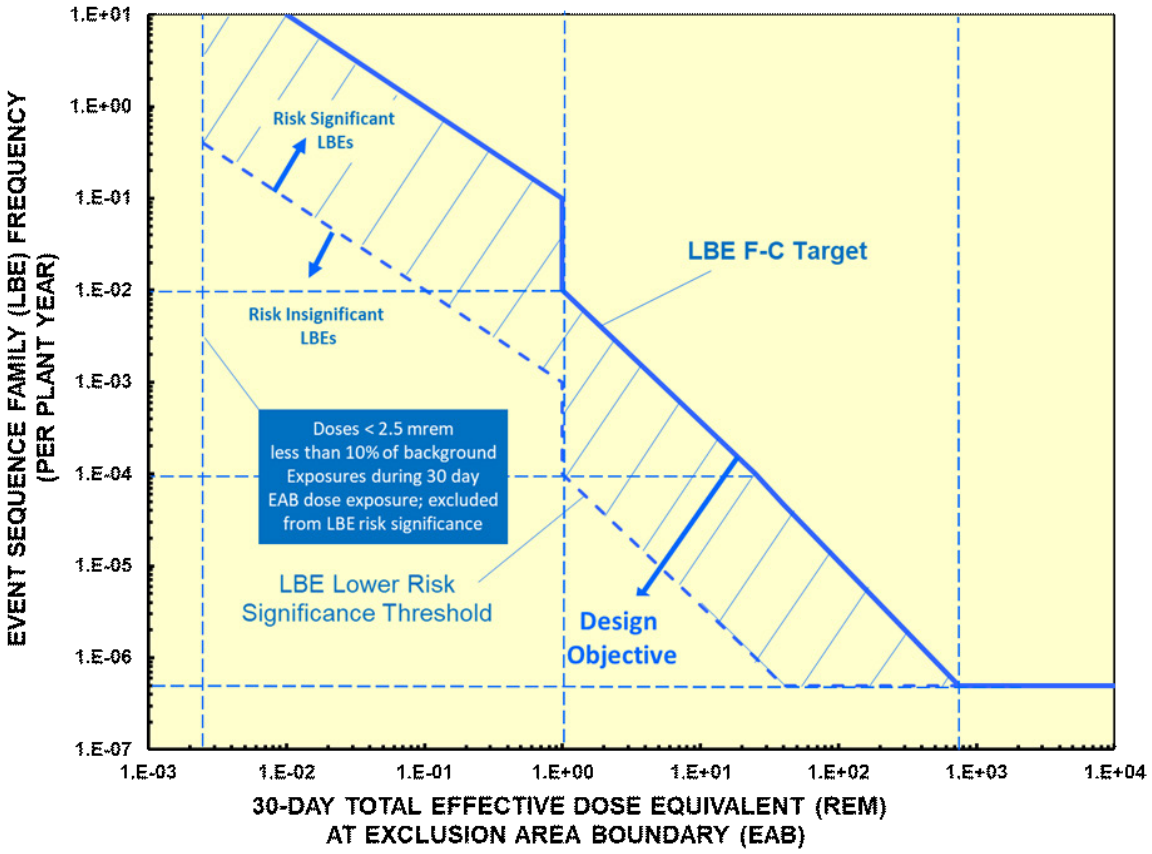


Figure 2-6. Use of F-C Target to Define Risk-Significant LBEs

Task 3. Define SSC Safety Functions for PRA Modeling

The plant designer defines the reactor-specific safety functions as represented in Task 3 for incorporation into the PRA, i.e. the PSFs. All reactors are designed to meet certain Fundamental Safety Functions (FSFs)* such as retention of radioactive material, control heat removal, and control of heat generation. However, application of the reactor-specific safety design approach leads to a set of reactor-specific PSFs that achieve the FSFs. During this process, the designer confirms the allocation of these PSFs to both passive and active SSCs. In Task 3, the top-level design criteria are also confirmed for all the SSCs selected to perform the reactor-specific PSFs. As Task 3 is completed, the plant capabilities that support DID are largely determined. Adjustments may be made to address the results of subsequent evaluations or design iterations that may expose weaknesses in design or operating assumptions or may 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 report, the definition of PSFs, defined as those functions responsible for the prevention and mitigation of release of radioactive material from

*The term "Fundamental Safety Function" is used extensively in IAEA publications such "Proposal for a Technology-Neutral Safety Approach for New Reactor Designs," Technical Report IAEA-TECDOC-1570. The functions listed are the ones regarded as fundamental and are applicable to all reactor technologies.

any radionuclide source in the scope of the PRA, and identification of SSCs that perform these functions is developed with close collaboration between development of the design and initial construction of the PRA model. These PSF 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 in evaluating DID adequacy.

Task 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 report, 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 with consideration of appropriate DID to address uncertainties and initial analysis results related to event frequencies and consequences. Depending on the stage of the design, the scope of the PRA may be extended to expand the range of hazards to be considered and the sources of radioactive material outside the reactor core that have their own unique safety functions, and SSCs to support those functions.

Task 5. Perform PRA

The performance of the current phase of the PRA is covered in this task consistent with the framework described in the LMP PRA report. As explained more fully in the PRA report, development and evaluation of the design and 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 RIPB evaluation of DID depicted in Tasks 12 and 17. As explained more fully in the supporting LMP report 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 in both LBE frequencies and consequences.

Task 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 report.

Task 7. Evaluate LBE Risks versus 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 the level of satisfaction of 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 task is discussed more fully in Section 2.9.

Task 8. Evaluate Plant Risks versus 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 report is also necessary to establish DID adequacy. This step is discussed more fully in Section 2.9.

Task 9. Identify DID Layers Challenged by Each LBE

The layers-of-defense framework in Figure 2-4 are used in this task 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 task is found in Section 2.9.

Task 10. Select SR SSCs and Define DBAs

As explained more fully in the LMP LBE report and LMP SSC report, 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 PSFs 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 (RSFs). In general, there may be two or more different sets of SSCs that could provide these RSFs. Those functions specified by the design team participating in the IDP select which of the available SSCs that can support the RSFs for all the DBEs and high-consequence BDBEs are designated as SR. DBAs are then constructed starting with each DBE and then assuming only the SR SSCs perform their associated RSFs. DID considerations are taken into account in the selection of SR SSCs by selecting those that yield high confidence in performing their RSFs 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 modular high-temperature gas-cooled reactor (MHTGR), a specific reactor designed by General Atomics, in the LMP LBE report.

Task 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 LWRs in this task. 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.

Task 12. Confirm Plant Capability DID Adequacy

At this task, there is sufficient information, even during the conceptual engineering phase, to evaluate the adequacy of the plant capabilities for DID using information from the previous tasks and guidelines for establishing the adequacy of DID as explained in Section 2.8. This task is supported by the results of the systematic evaluation of LBEs using the layers-of-defense process outlined in Figure 2-4 in Task 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.

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

As explained more fully in the LMP SSC report, 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. SSCs not classified as SR or NSRST are classified as non-SR 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. Those NST SSCs that are modeled in the PRA are found not to meet the risk significance thresholds. Those NST SSCs that are not modeled in the PRA are excluded only because it was demonstrated that risk significance thresholds would not be achieved, according to the requirements in the non-LWR PRA Standard.[16] All NST SSCs are classified as such because the DID evaluation did not identify they served any function required for DID adequacy. All of the safety-significant SSCs are classified as either SR or NSRST.

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

Also explained in the LMP SSC report is the definition of Required Functional Design Criteria (RFDC) for SR SSCs. RFDC provides 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 RSFs are used in the formulation of RFDC.

Task 15. Evaluate Uncertainties and Margins

One of the primary motivations for 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 that are not sufficiently characterized for uncertainty quantification nor amenable to sensitivity analyses. The plant capability DID includes design margins that protect against uncertainties. The layers of defense within a design, including Layer 5, offsite 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.

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

According to the SSC classification approach described in the LMP SSC report, 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 PSF with significant margins and with a high degree of reliability. These include numerical targets for SSC reliability and availability, design margins for performance of PSFs, 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 Task 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 during 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 report.

Task 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 Task 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.

Task 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 can make a practical, significant improvement to the LBE risk profiles or risk significant reductions in the level of uncertainty in characterizing the LBE frequencies and consequences. At this point, a DID baseline can be finalized to support the final design and operations of the plant.

The successful outcomes of Tasks 12 and 17 establish DID adequacy. This determination is made during 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 the remainder of this section and in Sections 3.3 and 3.5.

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

As seen in Table 2-1, there are important DID roles in each major element of the process. The IDP uses information and insights in each of these elements to support an RIPB evaluation of DID adequacy. As indicated in Figure 2-3, RIPB decisions that are made in this evaluation feed back 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.

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 IEs 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 of offsite radiological consequences Assessment of the IE frequencies, reliabilities, and availabilities of SSCs required to respond to those IEs 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 IE 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 SR 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 RFDC Selection of design requirements for SR SSCs Selection of performance-based reliability, availability, and capability targets for safety-significant SSCs Selection of special treatment requirements for safety-significant SSCs

Elements of TI-RIPB Framework	Role in Establishing DID Adequacy
Risk-informed evaluation of DID adequacy	Evaluation of DID attributes for DID Input to identification of safety-significant SSCs Input to selection of SR SSCs Evaluation of roles of SSCs in the prevention and mitigation of LBEs Evaluation of 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

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 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 SR equipment is a sensitivity study with additional conservatism built into 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 application of actions such as independent review and oversight programs. Applications of programs such as quality assurance (QA) programs, offsite 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 initial plant capability DID is established in the formulation of the reactor safety design approach, which is developed in a coordinated fashion with development of the plant PRA, as discussed more fully in the LMP PRA report. The plant capability DID is also influenced in the course of selecting and evaluating LBEs and in the safety classification of SSCs.

The process for establishing plant capability DID begins in the development of the safety design approach and is accomplished in the course of the iterative process tasks leading up to the selection and evaluation of the LBEs as shown in Figure 2-7 and is also impacted by the SSC safety classification. Task 7e in Figure 2-7 represents the task in the LBE evaluation in which the plant capability for DID is assessed. Information developed in the LBE selection and evaluation process is also used to support SSC safety classification as shown in Figure 2-8 that 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 this process, a set of DID adequacy guidelines has been developed. The guidelines, presented in Figure 2-7, can be used as a basis for initially evaluating the adequacy of plant capability DID and are confirmed during the regulatory review as appropriate and sufficient.

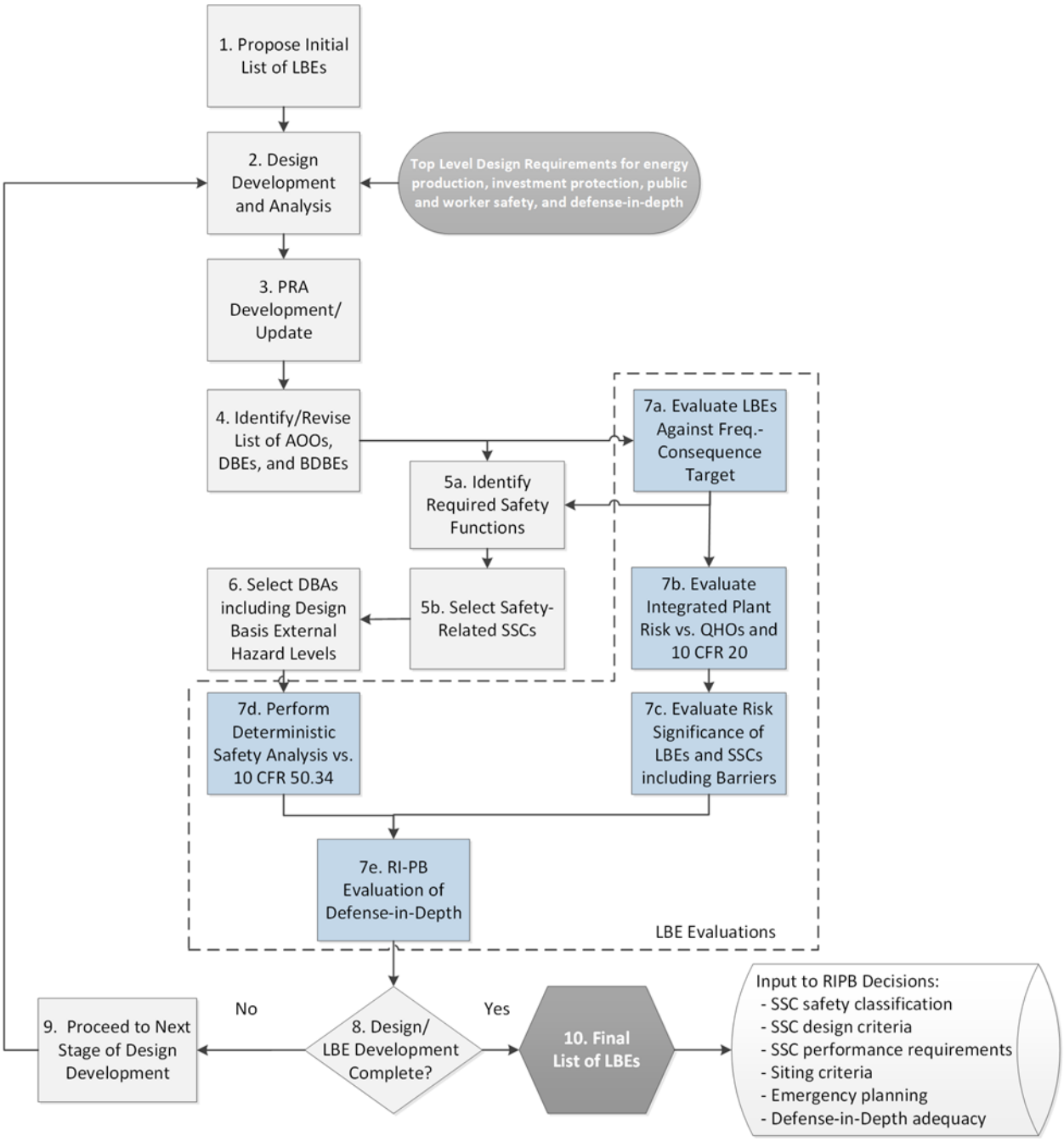


Figure 2-7. LMP Process for Selecting and Evaluating LBEs

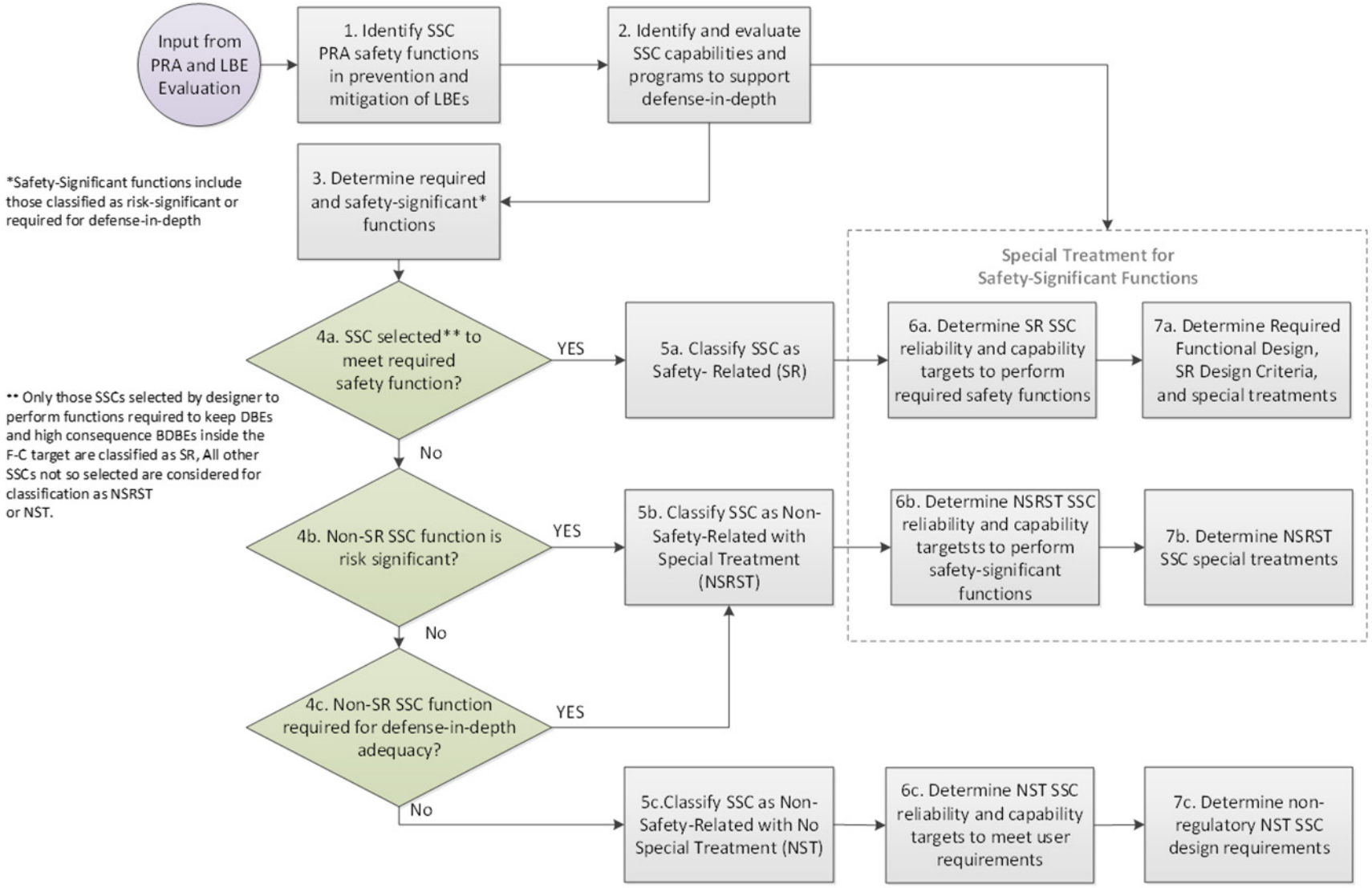


Figure 2-8. LMP Approach to the Safety Classification of SSCs and Formulation of SSC Performance Requirements

Table 2-2. Guidelines for Establishing the Adequacy of Overall Plant Capability DID

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

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 IEs 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 Tasks 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. Safety significant SSCs are classified as SR if they have been selected to perform an RSF. The remaining safety significant SSCs are classified as NSRST. The plant capability DID adequacy guidelines in Table 2-2 are used in part to guide the IDP in identifying non-SR SSC functions that must be preserved to provide an adequate level of defense-in-depth. This evaluation may or may not lead to additional SSCs being classified as NSRST.

The third and fifth column of this table require that two or more independent plant design or operational features be provided to meet the quantitative guidelines in Columns 2 and 4 of the table. The design features considered in the evaluation for this table include inherent plant features that support the performance of passive safety functions modeled in the LBEs as well as active SSCs that perform the LBE safety functions. The operational features considered in this evaluation include human actions that support safety functions as well as programmatic measures to ensure adequate reliability and capability of SSCs that perform safety functions. Results from the evaluations against these criteria performed during the IDP are considered as one input to decisions that may or may not result in classifying additional SSCs as NSRST, as explained more fully below.

As an example, consider the qualitative criterion in Column 3 in Layer 3. Evaluating this part of the table would involve reviewing all the BDBEs to identify whether the frequency of each BDBE is relying on a single design or operational feature to keep its frequency below 10^{-4}/plant-year. If this is true, the margins between the frequency and consequences of the affected BDBE and the F-C target are identified in evaluating the Column 4 criteria. The actual decision regarding whether these evaluations lead to any SSC classification as NSRST are made on a case by case basis depending on whether any special treatments would have any significant impact on LBE risks.

Sensitivity analyses may be performed to evaluate the risk impact of removing one or more design or operational features that are reflected in the LBEs in applying these criteria. It is appropriate that for the inherent capabilities of passive functions, degradation of the passive function is considered, as opposed to complete failure (i.e., a physical non-existence of that function). As degradation or failure of plant design or operational features are analyzed against the quantitative guidelines in Table 2-2, the analysis should be kept in the context of risk added from these plant disruptions (i.e., certain LBEs may exceed the frequency thresholds but not carry any consequence).

The IDP may determine whether additional requirements on SSCs (e.g., elevating classification) or other operational programs are needed to meet the Table 2-2 guidelines. The IDP may also determine that no further design requirements or operational programs are needed, or that previously identified requirements and operational programs are no longer needed to assure DID adequacy. 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 SR nor risk significant, the IDP could classify the SSC as safety-significant and NSRST if it performs a function required for DID adequacy according to the guidelines in Table 2-2 and if the resulting special treatment would have a significant cost benefit and effective risk impact on the affected LBEs.

For addition discussion on the evaluation of low or no dose LBEs (e.g. “zero consequence”) using Plant Capability Guidelines of Table 2-2, see Appendix A.

As explained more fully in the LMP SSC report, 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 3.0.

The quantitative criteria in Column 3 of this table are not intended to constrain design changes made in successive iterations of the design evolutions. As explained more fully in Section 2.5 each time a design change is made, it is necessary to revisit the steps in the LMP methodology including those associated with LBE selection and evaluation, and SSC classification up to and including a "fresh look" at the criteria in Table 2-2. In the case of evaluating such design changes, where risk is not increased as a result of a frequency increase, additional requirements on SSC classification or other operational solutions may not be needed and requirements added in previous design iterations may no longer be needed.

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 supports making an appropriate safety case and ultimate finding that a plant poses no undue risk to 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 DID Attributes

Attribute	Evaluation Focus
IE and accident sequence completeness	PRA documentation of IE selection and event sequence modeling Insights from reactor operating experience, system engineering evaluations, and 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

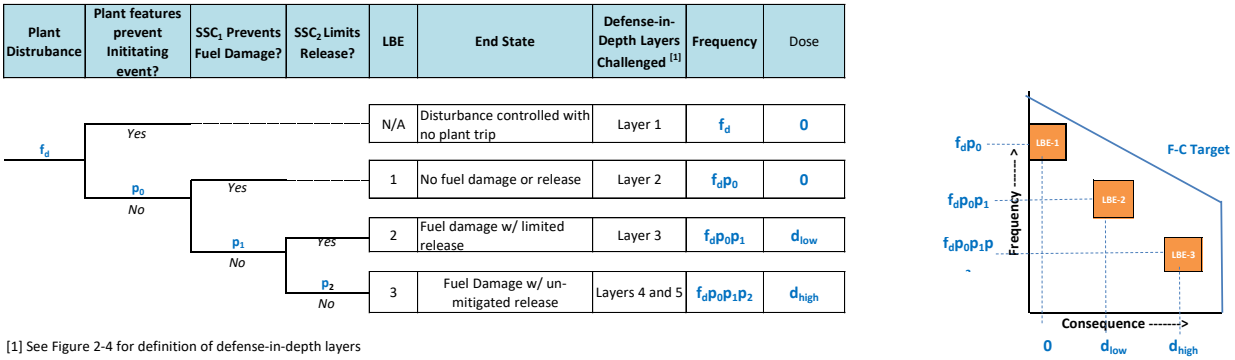
A central element of the RIPB evaluation of DID is a systematic review of the LBEs against the layers of defense. This review by the IDP is necessary to evaluate the plant capabilities for DID and to identify any programmatic DID measures that may be necessary for establishing DID adequacy. In meeting its objectives, the review will:

- Confirm that plant capabilities for DID are deployed to prevent and mitigate each LBE at each layer of defense challenged by the LBE.
- Confirm that a balance between accident prevention and mitigation is reflected in the layers of defense for risk-significant LBEs.
- Identify the reliability/availability missions of SSCs that perform prevention and mitigation functions along each LBE and confirm that these missions can be accomplished. A reliability/availability mission is the set of requirements related to the performance, reliability, and availability of an SSC function that adequately ensures the accomplishment of its task, as defined by the PRA or deterministic analysis.
- Confirm that adequate technical bases for classifying SSCs as SR or NSRST exist and their capabilities to execute the required safety functions are defined.
- Confirm that the effectiveness of physical and functional barriers to retain radionuclides in preventing or limiting release is established.

- 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.
- Confirm that risk-significant sources of uncertainty in both the frequency and consequence estimates that need to be addressed via programmatic and plant capability DID measures have been adequately addressed.

As explained more fully in the LMP SSC report, 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 important 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 IE, and two sets of SSCs that have the capability to prevent or mitigate an accident.



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 DID

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

*LBEs with site boundary doses exceeding 1 rem (total effective dose equivalent), the lower Environmental Protection Agency Protective Action Guideline dose, are regarded as having relatively high consequences for this purpose.

response to the IE. 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 IE 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.

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 IE is an event that 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 PSFs 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 PSFs, 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 based on the IEs 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, coolant pressure boundary, and 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 should 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

*In this document, 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.

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 plant release.

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 table provides an important feedback mechanism between RIPB 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
IE occurrence	Reliability of SSCs supporting power generation reduces the IE frequencies; successful operation of these SSCs prevents the sequence.	Capabilities of normally operating systems to continue operating during disturbances to prevent IEs 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 IEs 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 IEs 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 methodology 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:

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

where:

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*

The above model was developed for a reactor having a fuel barrier, reactor pressure boundary barrier, and a reactor building barrier. This model would need to be revised for applicability to different reactor barrier configurations.

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 DBE 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 cooldown 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 DBE but with a lower frequency and higher potential for release than in Sequence 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 cooldown 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 MHTGR-2). This sequence is representative of a BDBE 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.

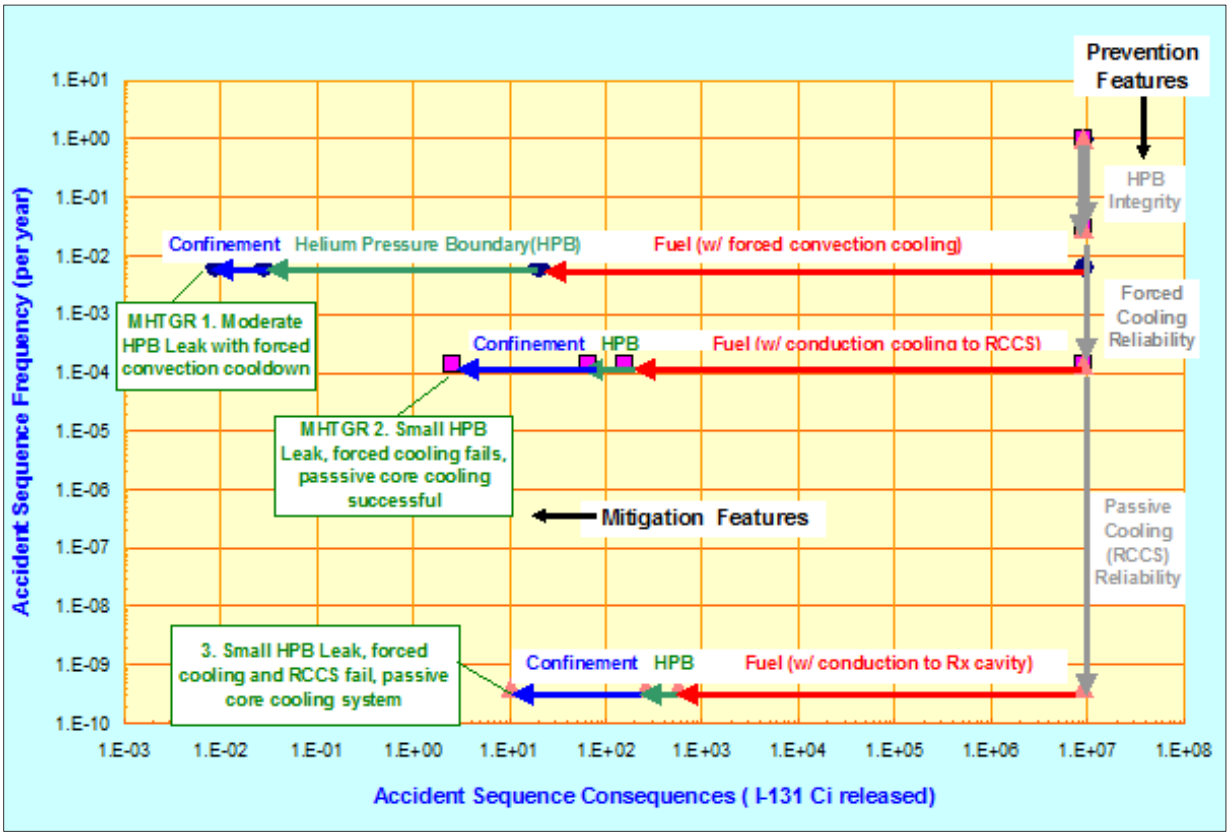


Figure 2-10. Example Evaluation of SSCs Responsible for Preventing and Mitigating MHTGR LBEs[2]

As seen in the figures, the roles of prevention and mitigation for Sequence MHTGR-1 include two 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.

Sequence 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 Sequence 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 MHTGR 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 methodology, all the risk-significant LBEs as well as the LBEs used to select the DBAs and to identify the risk-significant SSCs are examined during 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 HPB leak), DBE-10 (large HPB 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}/plant-year to 0.025/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]	Mean 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).

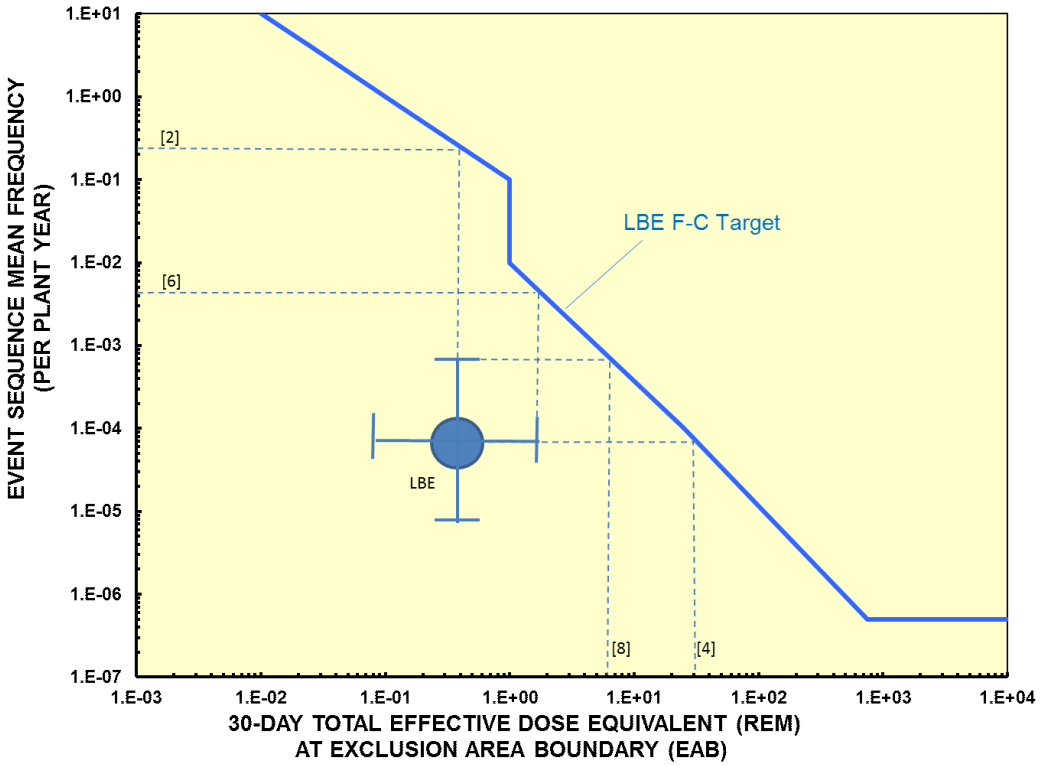


Figure 2-11. Guidance for Defining Margins Between LBE Frequencies and Doses Relative to the F-C Target

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. This process is repeated for each individual LBE, grouped by LBE category as part of the DID evaluation during the design development.

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] The limiting LBE is the LBE with the highest risk significance in the 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 dose margins range from 500 to 60,000 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 design development.

2.9.2 Integrated Decision Process Focus in LBE Review

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

- Is the selection of IEs 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 RSFs adequate?
- Is the selection of the SR SSCs to perform the RSFs 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 IEs 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 task 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 that 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)
Offsite 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 addressed for each programmatic DID attribute for risk-significant LBEs to determine that the programmatic DID provides sufficient confidence that public health and safety based on the design plant capability can be achieved throughout the plant lifetime. 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 are used during the IDP.

Table 2-8. Evaluation Considerations for Evaluating Programmatic DID Attributes

Evaluation Focus	Implementation Strategies	Evaluation Considerations
Quality / Reliability Attribute		
Design Testing Manufacturing Construction O&M	Conservatism with bias to prevention Equipment codes and standards Equipment qualification Performance testing	1. Is there appropriate bias to prevention of AOOs progressing to postulated event sequences? 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 SR SSCs been properly classified for special treatment consistent with their risk significance?
Compensation for Uncertainties Attribute		
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?

Evaluation Focus	Implementation Strategies	Evaluation Considerations
Compensation for mechanical errors	Operational technical specifications Allowable outage times Part 21 reporting Maintenance rule scope	1. Are all risk-significant LBE limiting condition for operation reflected in plant operating technical specifications? 2. Are allowable outage times in technical specifications consistent with assumed functional reliability levels for risk-significant LBEs? 3. Are all risk-significant SSCs properly included in the maintenance program?
Compensation for unknowns (performance variability)	Operational technical specifications In-service monitoring programs	1. Are the technical specifications 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 events 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?
Offsite Response Attribute		
Emergency response capability	Layers of Response Strategies Emergency Planning Zone Location Emergency Planning 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 emergency planning 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 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 where 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 during 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 report on SSC safety classification, graded QA should be applied to NSRST SSCs based on the layer of defense and for risk-significant SSC PSFs.

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 also evaluated as part of Programmatic DID adequacy. At the individual SSC level, properly designing SSCs to proven codes and standards provides an appropriate, conservative 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?" and "What are the consequences?" should become institutionalized as a part of deciding how to manage residual risk and uncertainty. The primary means to address these residual risks is through effective Severe Accident Management Programs and effective emergency planning. Siting considerations and emergency planning zone programs take into account the known risks of a plant, siting the plant in less populated

areas and incorporating proactive emergency planning programs that ensure precautionary actions are taken well before a serious threat to public health can arise.

Compensation for Unknowns

The layers-of-defense approach utilized in the DID evaluation process 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. Relevant, known nuclear industry sources of information should be utilized for known, risk-significant LBEs. The PRA standard has requirements for accounting for all relevant sources of information for all modeled event sequences but there are more stringent requirements for risk significant event sequences.

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
- Design certification application/combined license application 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 inspections 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 during 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 sufficient confidence in the predicted safety performance of the plant throughout its lifetime.

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 startup programs	Equipment fabrication oversight Construction oversight Factory testing and qualification Startup 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
QA 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	Owner-directed independent reviews and performance monitoring programs
Equipment qualification programs	Seismic qualification Adverse environment qualification Physical protection
Emergency planning programs	Periodic drills Emergency response equipment maintenance programs

There are other programmatic activities spread across a broader portion of the industry that provide additional levels of programmatic DID and contribute to assurance of public protection.

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 RIPB EVALUATION OF DID ADEQUACY

3.1 Purpose and Scope of IDP Activities

In the LMP methodology, an IDP is utilized for evaluating the adequacy of DID. How the process is implemented may vary depending on the state of design development, construction or operations. It may be done integral to the design control process, like many other technical decisions or as part of a panel (IDPP) as is done with operational phase reviews. 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 that 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 tasks for evaluating DID shown in Figure 2-5. The process includes those responsible for the design, operations, and maintenance program development and for performing the necessary deterministic and probabilistic evaluations identified in this figure.

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] 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.

3.2 Risk-Informed and Performance-Based Decision-Making Process

The IDP will use an RIPB 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 central 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 2.0.

Table 3-1 lists 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. RIPB 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 performance-based 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 tasks 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.
- A decision made collaboratively by knowledgeable, responsible individuals based on the defined attribute evaluation requirements
- If compensatory actions are needed, identification of potential plant capability and/or programmatic choices
- Implementation closure of DID open actions and documentation of the results of the RIPB-DM process and rationale for the decisions in a record appropriate for the stage of the design process

A 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 IEs 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) 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 the 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 as early means to resolve operational challenges. It is during this period of design development, that 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 the plant and system levels.

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 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 onsite 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 LBEs 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 IEs that can progressively cascade to the point of challenging public safety objectives. IEs 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 BDBEs, 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 that could be impractical to implement or excessively burdensome. Small changes to the design that improve the likelihood of successful actions should be considered 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 emergency preparedness DID alone.

3.5 Baseline Evaluation of DID

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 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 tasks 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 that will be recorded 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			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 is derived from the design records, primarily those that verified the attributes described in Section 2 were adequate. The development of the baseline should support and complement existing change control requirements such as 10 CFR 50.59 where the impact on DID is considered. 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 the DID attributes as described in Section 2.0 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 appropriate DID attributes are in place commensurate with the identified event risks.

3.7 Evaluation of Changes to DID

For each iteration of the design evaluation lifecycle in Figure 2-5, the DID evaluation from the baseline will be reevaluated based on a review to determine which programmatic or plant capability attributes have been affected for each layer of defense. 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 reevaluated and the baseline updated as appropriate.

4.0 GLOSSARY OF TERMS

LMP Term	Acronym	Definition	Source
Terms Associated with Functions			
Fundamental Safety Function	FSF	Safety functions common to all reactor technologies and designs; includes control heat generation, control heat removal and confinement of radioactive material	IAEA-TECDOC-1570
PRA Safety Function	PSF	Reactor design specific SSC functions modeled in a PRA that serve to prevent and/or mitigate a release of radioactive material or to protect one or more barriers to release. In ASME/ANS-Ra-S-1.4-2013 these are referred to as "safety functions." The modifier PRA is used in the LMP GD to avoid confusion with safety functions performed by Safety-Related SSCs.	LMP, ASME/ANS-Ra-S-1.4-2013
Prevention Function	--	An SSC function that, if fulfilled, will preclude the occurrence of an adverse state. The reliability of the SSC in the performance of such functions serves to reduce the probability of the adverse state.	LMP
Mitigation Function	--	An SSC function that, if fulfilled, will eliminate or reduce the consequences of an event in which the SSC function is challenged. The capability of the SSC in the performance of such functions serves to eliminate or reduce any adverse consequences that would occur if the function were not fulfilled.	LMP
Required Safety Function	RSF	A PRA Safety Function that is required to be fulfilled to maintain the consequence of one or more DBEs or the frequency of one or more high-consequence BDBEs inside the F-C Target	LMP
Required Functional Design Criteria	RFDC	Reactor design-specific functional criteria that are necessary and sufficient to meet the RSFs	LMP
Safety-Related Design Criteria	SRDC	Design criteria for SR SSCs that are necessary and sufficient to fulfill the RFDCs for those SSCs selected to perform the RSFs	LMP
Terms Associated with Licensing Basis Events			
Anticipated Operational Occurrence	AOO	Anticipated event sequences expected to occur one or more times during the life of a nuclear power plant, which may include one or more reactor modules. Event sequences with mean frequencies of 1×10^{-2}/plant-year and greater are classified as AOOs. AOOs take into account the expected response of all SSCs within the plant, regardless of safety classification.	LMP

LMP Term	Acronym	Definition	Source
Design Basis Event	DBE	Infrequent event sequences that are not expected to occur in the life of a nuclear power plant, which may include one or more reactor modules, but are less likely than AOOs. Event sequences with mean frequencies of 1×10^{-4}/plant-year to 1×10^{-2}/plant-year are classified as DBEs. DBEs take into account the expected response of all SSCs within the plant regardless of safety classification. The objective and scope of DBEs form the safety design basis of the plant.	LMP
Beyond Design Basis Event	BDBE	Rare event sequences that are not expected to occur in the life of a nuclear power plant, which may include one or more reactor modules, but are less likely than a DBE. Event sequences with frequencies of 5×10^{-7}/plant-year to 1×10^{-4}/plant -year are classified as BDBEs. BDBEs take into account the expected response of all SSCs within the plant regardless of safety classification.	LMP
Design Basis Accident	DBA	Postulated accidents that are used to set design criteria and performance objectives for the design of Safety-Related SSCs. DBAs are derived from DBEs based on the capabilities and reliabilities of Safety-Related SSCs needed to mitigate and prevent accidents, respectively. DBAs are derived from the DBEs by prescriptively assuming that only SR SSCs classified are available to mitigate postulated accident consequences to within the 10 CFR 50.34 dose limits.	LMP
Licensing Basis Event	LBE	The entire collection of event sequences considered in the design and licensing basis of the plant, which may include one or more reactor modules. LBEs include AOOs, DBEs, BDBEs, and DBAs.	LMP
Frequency-Consequence Target	F-C Target	A target line on a frequency-consequence chart that is used to evaluate the risk significance of LBEs and to evaluate risk margins that contribute to evidence of adequate defense-in-depth	LMP
Risk-Significant LBE	--	An LBE whose frequency and consequence meet a specified risk significance criterion. In the LMP framework, an AOO, DBE, or BDBE is regarded as risk-significant if the combination of the upper bound (95%tile) estimates of the frequency and consequence of the LBE are within 1% of the F-C Target AND the upper bound 30-day TEDE dose at the EAB exceeds 2.5 mrem.	LMP
Terms Associated with Plant Design and Structures, Systems, and Components			
Design Basis External Hazard Level	DBEHL	A design specification of the level of severity or intensity of an external hazard for which the Safety-Related SSCs are designed to withstand with no adverse impact on their capability to perform their RSFs	LMP
Plant		The collection of site, buildings, radionuclide sources, and SSCs seeking a single	LMP

LMP Term	Acronym	Definition	Source
		design certification or one or more operating licenses under the LMP framework. The plant may include a single reactor unit or multiple reactor modules as well as non-reactor radionuclide sources.	
Multi-Reactor Module Plant	--	A plant comprising multiple reactor modules that are designed and constructed using a modular design approach. Modular design means a nuclear power plant that consists of two or more essentially identical nuclear reactors (modules) and each reactor module is a separate nuclear reactor capable of being operated independent of the state of completion or operating condition of any other reactor module co-located on the same site, even though the nuclear power plant may have some shared or common systems.	Multi-module plant adapted from ASME/ANS-Ra-S-1.4-2013, modular design from 10 CFR 52.1
Safety-Related SSCs	SR SSCs	SSCs that are credited in the fulfillment of RSFs and are capable to perform their RSFs in response to any Design Basis External Hazard Level	LMP
Non-Safety-Related with Special Treatment SSCs	NSRST SSCs	Non-safety-related SSCs that perform risk-significant functions or perform functions that are necessary for defense-in-depth adequacy	LMP
Non-Safety-Related with No Special Treatment SSCs	NST SSCs	All SSCs within a plant that are neither Safety-Related SSCs nor Non-Safety-Related SSCs with Special Treatment SSCs	LMP
Risk-Significant SSC	--	An SSC that meets defined risk significance criteria. In the LMP framework, an SSC is regarded as risk-significant if its PRA Safety Function is: a) required to keep one or more LBEs inside the F-C Target based on mean frequencies and consequences; or b) if the total frequency LBEs that involve failure of the SSC PRA Safety Function contributes at least 1% to any of the LMP cumulative risk targets. The LMP cumulative risk targets include: (i) maintaining the frequency of exceeding 100 mrem to less than 1/plant-year; (ii) meeting the NRC safety goal QHO for individual risk of early fatality; and (iii) meeting the NRC safety goal QHO for individual risk of latent cancer fatality.	LMP
Safety-Significant SSC	--	An SSC that performs a function whose performance is necessary to achieve adequate defense-in-depth or is classified as Risk-Significant (see Risk-Significant	LMP

LMP Term	Acronym	Definition	Source
		SSC).	
Safety Design Approach	--	The strategies that are implemented in the design of a nuclear power plant that are intended to support safe operation of the plant and control the risks associated with accidental releases of radioactive material and protection of the public and plant workers. These strategies normally include the use of robust barriers, multiple layers of defense, redundancy, and diversity, and the use of inherent and passive design features to perform safety functions.	LMP
Terms Associated with Risk-Informed and Performance-Based Regulation and Decision-Making			
Defense-in-Depth	DID	"An approach to designing and operating nuclear facilities that prevents and mitigates accidents that release radiation or hazardous materials. The key is creating multiple independent and redundant layers of defense to compensate for potential human and mechanical failures so that no single layer, no matter how robust, is exclusively relied upon. Defense-in-depth includes the use of access controls, physical barriers, redundant and diverse key safety functions, and emergency response measures."	NRC Glossary
Layers of Defense	--	Layers of defense are those plant capabilities and programmatic elements that provide, collectively, independent means for the prevention and mitigation of adverse events. The actual layers and number are dependent on the actual source and hazard posing the threat. See Defense-in-Depth.	LMP
Performance-Based	PB	An approach to decision-making that focuses on desired objective, calculable or measurable, observable outcomes, rather than prescriptive processes, techniques, or procedures. Performance-based decisions lead to defined results without specific direction regarding how those results are to be obtained. At the NRC, performance-based regulatory actions focus on identifying performance measures that ensure an adequate safety margin and offer incentives and flexibility for licensees to improve safety without formal regulatory intervention by the agency.	Adapted from NRC Glossary definition of performance-based regulation in order to apply to both design decisions and regulatory decision-making
Risk-Informed	RI	An approach to decision-making in which insights from probabilistic risk assessments are considered with other sources of insights	Adapted from NRC Glossary definition of performance-based regulation in order to apply to both design decisions and regulatory decision-making
Risk-Informed	RIPB-DM	The union of risk information and performance information to achieve performance-	

LMP Term	Acronym	Definition	Source
and Performance-Based Integrated Decision-Making		based objectives	
Terms Associated with Probabilistic Risk Assessment			
Initiating Event	IE	A perturbation to the plant during a plant operating state (POS) that challenges plant control and safety systems whose failure could potentially lead to an undesirable end state and/or radioactive material release. An Initiating Event could degrade the reliability of a normally operating system, cause a standby mitigating system to be challenged, or require that the plant operators respond in order to mitigate the event or to limit the extent of plant damage caused by the Initiating Event. These events include human-caused perturbations and failure of equipment from either internal plant causes (such as hardware faults, floods, or fires) or external plant causes (such as earthquakes or high winds). An Initiating Event is defined in terms of the change in plant status that results in a condition requiring shutdown or a reactor trip (e.g., loss of main feedwater system, small reactor coolant pressure boundary [RCPB] breach) when the plant is at power, or the loss of a key safety function (e.g., decay heat removal system) for non-power modes of operation. A specific type of Initiating Event may be identified as originating from a specific cause as defined in terms such as "flood-induced transient" or "seismically-induced RCPB breach."	ASME/ANS-Ra-S-1.4-2013
Event Sequence	ES	A representation of a scenario in terms of an Initiating Event defined for a set of initial plant conditions (characterized by a specified POS) followed by a sequence of system, safety function, and operator failures or successes, with sequence termination with a specified end state (e.g., prevention of release of radioactive material or release in one of the reactor-specific release categories. An event sequence may contain many unique variations of events (minimal cut sets) that are similar in terms of how they impact the performance of safety functions along the event sequence.	ASME/ANS-Ra-S-1.4-2013
Event Sequence	-	A grouping of event sequences with a common or similar POS, Initiating Event, hazard group, challenges to the plant safety functions, response of the plant in the	

LMP Term	Acronym	Definition	Source
Family		performance of each safety function, response of each radionuclide transport barrier, and end state. An event sequence family may involve a single event sequence or several event sequences grouped together. Each release category may include one or more event sequence families. Event sequence families are not required to be explicitly modeled in a PRA. Each event sequence family involving a release is associated with one and only one release category.	
End State		The set of conditions at the end of an Event Sequence that characterizes the impact of the sequence on the plant or the environment. In most PRAs, end states typically include success states (i.e., those states with negligible impact) and Release Categories.	ASME/ANS-Ra-S-1.4-2013
PRA Technical Adequacy	--	A set of attributes that define the technical suitability of a PRA capability to provide fit-for-purpose insights to risk-informed decision-making. It includes consideration of realism, completeness, transparency, PRA model-to-plant as-designed and as-built fidelity state, and identification and evaluation of uncertainties relative to risk levels. Strategies to achieve technical adequacy include conformance to consensus PRA standards, performance of PRA peer reviews, and structured processes for PRA model configuration control, maintenance and updates, and incorporation of new evidence that comprises the state of knowledge reflected in the PRA model development and its quantification.	LMP
Plant Operating State	POS	A standard arrangement of the plant during which the plant conditions are relatively constant, are modeled as constant, and are distinct from other configurations in ways that impact risk. POS is a basic modeling device used for a phased-mission risk assessment that discretizes the plant conditions for specific phases of an LPSD evolution. Examples of such plant conditions include core decay heat level, primary coolant level, primary temperature, primary vent status, reactor building status, and decay heat removal mechanisms. Examples of risk impacts that are dependent on POS definition include the selection of Initiating Events, Initiating Event frequencies, definition of accident sequences, success criteria, and accident sequence quantification.	ASME/ANS-Ra-S-1.4-2013
Mechanistic Source Term	MST	A source term that is calculated using models and supporting scientific data that simulate the physical and chemical processes that describe the radionuclide inventories and the time-dependent radionuclide transport mechanisms that are necessary and sufficient to predict the source term.	ASME/ANS-Ra-S-1.4-2013

5.0 REFERENCES

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

[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 and Evaluation of Licensing Basis Events," Rev 1, March 2020.

[10] Idaho National Laboratory, "Modernization of Technical Requirements for Licensing of Advanced Non-Light Water Reactors, Probabilistic Risk Assessment Approach Rev 1, March 2020.

[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," Rev 1, March, 2020.

[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, Technical Report IAEA-TECDOC-1570, "Proposal for a Technology-Neutral Safety Approach for New Reactor Designs," ISBN 978–90–0–107607–6, September 2007.

[19] Nuclear Energy Institute, NEI 18-04 "Risk-Informed Performance-Based Technology Inclusive Guidance for Advanced Reactor Licensing Basis Development," Revision 0, April 1, 2019.

[20] U.S. Nuclear Regulatory Commission, "NRC Staff Comments/Questions on LMP White Paper on PRA Approach," ADAMS Accession No. ML17233A187, August 18, 2017.

[21] U.S. Nuclear Regulatory Commission, "NRC Staff Comments and Questions, Licensing Modernization Project: Evaluation of Defense-in-Depth Adequacy," ADAMS Accession No. ML18024A595, January 19, 2018.

APPENDIX A—TABLE 2-2 INTERPRETATION OF PLANT CAPABILITY DID GUIDELINES

Background

The concept of DID is well established in NRC philosophy, even if not by line item regulation, and must be reflected in any application regardless of licensing framework chosen by the designer. The risk-informed, performance-based LMP process is intended to guide designers through a systematic examination of the risk-informed need for DID and appropriate designer-chosen actions. The LMP Team considered the text of NEI 18-04 and as a team concluded that the guidance is appropriate for that need and that the designer, via the designer's own integrated decision-making process (IDP), has broad flexibility in choosing how to address DID for their particular design – including the option to do nothing if there isn't a RIPB need or the alternatives are of minimal risk reduction value or impractical. NEI 18-04 guidance encourages designers to consider a wide variety of both plant capability and programmatic capability options to ensure adequate DID; the IDP should ensure that options which add burden disproportionate to the risk and safety benefit sought are avoided. It is incumbent on the designer to make the decisions regarding DID that will be reflected in the application submitted to the NRC and defended by the designer during the NRC review process.[*]

During the GE-Hitachi (GEH) LMP tabletop presentation, a generic question arose about the defense-in-depth (DID) adequacy guidelines in Table 5-2 of NEI 18-04.[†] In the limited time available for the DID part of the RIPB demonstration project, GEH chose to focus on application of the guidelines in Table 5-2 for addressing the adequacy of Plant Capability DID. In the demonstration, GEH identified several SSCs that could be classified as NSRST for the heat removal required safety function as a means of fulfilling the DID adequacy guidelines. Options other than classifying SSCs as NSRST that could be identified with a more complete execution of all of the DID methodology parts that were not explored as they were outside the scope of the demonstration.

Specific responses to the direct and indirect questions arising from this issue are provided below along with a generic example at the end that illustrates how this aspect of DID can be evaluated for a single initiating event tree of LBEs.

Question 1: Why does LMP include a DID adequacy criterion in Table 5-2 to maintain the frequency of DBEs in the DBE region (Layer 2 quantitative guideline) and why is it reasonable to have this criterion even if the affected DBEs have zero consequence?

Response

A complete evaluation of DID adequacy contains three parts—the evaluation of Plant Capability, the evaluation of Programmatic actions and the Integrated Decision Process that evaluates sources and significance of residual uncertainties with the plant design and programs.

[*] These objectives are analogous to those contained in R.G. 1.74 Rev. 3 regarding using RIPB processes to change the licensing basis of a plant.

[†] To provide a context for the question, it is noted that due to constraints on available resources to support the tabletop. This prevented the full execution of the DID aspects of the LMP methodology.

Compensatory actions, such as safety classification changes, based on the evaluation of DID adequacy should only be proposed after completion of the whole DID evaluation process.

The purpose of the guidelines in Table 5-2 is not to determine the risk significance of LBEs but rather to address the adequacy of the plant capabilities DID that include considerations that extend beyond the evaluation of LBE frequencies and consequences alone. The evaluation of risk significance of LBEs using comparisons against the F-C Target and cumulative risk targets is part of the LBE selection and evaluation tasks that precede the application of Table 5-2. DID adequacy is achieved by ensuring that both quantitative and deterministic qualitative criteria have been adequately addressed including those in Table 5-2. DBEs, including those that have zero consequences, play an important role in determining the Required Safety Functions necessary to keep the DBEs inside the F-C target; in evaluating SSC risk-significance, safety classification and special treatment; and, in evaluating whether there is overreliance on a single feature in the design. Column 4 of Table 5-2 considers whether there are adequate margins between the LBE risks and the risk targets. The remaining columns in this table go beyond the examination of risk significance of LBEs to determine whether additional quantitative and qualitative guidelines have been adequately addressed as part of establishing Plant Capabilities for DID adequacy. These criteria provide a means of incorporating deterministic aspects into risk-informed decision making regarding plant capability.

The specific question arose on the guidelines in Layer 2 of Table 5-2 that are used to control the frequency of DBEs to ensure they remain less than 10^{-2}/plant-year. The underlying questions include: why is there a need to control DBE frequencies even if a DBE has zero consequences and whether a zero (low) dose DBE should require non-safety related SSC to be classified as NRSRT to keep the DBE frequency in the DBE region. The rationale for examining zero dose DBE is based in part on the second guideline, “Minimize frequency of challenges to SR SSCs” and in part on the level 3 guideline, “No single design or operational feature relied upon to meet quantitative objective for all DBEs.” The first quantitative guideline attached to this is simply to keep the DBEs inside the DBE region, i.e., to not let them move into the AOO region. RSFs are those functions that are necessary to keep the DBEs inside the F-C target. If SR SSCs are involved in a DBE, by minimizing the frequency of challenging the SR SSCs in Layer 2 we are helping to preserve the design basis objective of having layers of defense with different levels of response available in a progressive manner and also preventing risk-significant BDBEs in the BDBE region. Given the fact that SR SSCs have a certain probability of failure, by reducing or keeping the frequency of challenges to SR SSCs lower, the goal of keeping the DBEs in the DBE region also serves to keep BDBEs in the BDBE region. That is true because for each DBE in which the SR SSCs are successful in mitigating the consequence of the DBE there are associated sequences in the BDBE region in which one or more SR SSCs are postulated to fail. By keeping the DBEs in the DBE region which contributes to keeping the BDBEs in the BDBE region, we are maintaining the design basis, maintaining the frequency of exceeding the design basis, and maintaining the technical basis for selecting the SR SSCs and defining the DBAs. It is also noted that many if not most DBEs have zero consequences as shown in the MHTGR and PRISM examples in the LBE white paper and GEH tabletop.

The quantitative criteria in Column 3 of this table are not intended to constrain design changes made in successive iterations of the design evolutions. As explained more fully in Section 2.5 each time a design change is made, it is necessary to revisit the steps in the LMP methodology including those associated with LBE selection and evaluation, and SSC classification up to and including a "fresh look" at the criteria in Table 2-2.

The other guideline regarding avoiding overreliance on a single feature should be evaluated as well. In the case of DBEs, regardless of dose, each DBE gets evaluated for overreliance on a single feature. The reason for this is to determine that if that feature fails (it may be non-safety related) and the next level of plant response would include a significant non-zero dose, then further evaluation of that feature is warranted by completing the evaluation of programmatic DID and the range of uncertainties and margins in the subsequent LBE as part of the integrated decision process for DID adequacy before concluding that additional compensatory action is needed or the nature of compensatory action to be taken.

A second reason for these Layer 2 guidelines for DID adequacy is associated with preserving the technical basis for selecting the DBAs and for deriving the reliability and capability requirements for SR SSCs. Each DBE has associated with it a corresponding DBA defined by taking the DBE and removing credit for any operating SSC that performs a RSF and is not a SR SSC. In addition, the reliability and capability requirements for SR SSCs are based on the challenges to the SR SSCs reflected in the DBEs. As we lose one or more DBEs because they migrated up into the AOO region we lose their associated DBAs and the role of those migrating DBEs in forming the SR SSC reliability and capability requirements is lost. Hence the completeness of the DBA selection process may be adversely affected by permitting DBEs to migrate into the AOO region, independent of the magnitude of the DBE consequences.

In summary, the guideline to keep the DBE frequencies below 10-2/plant-year is based on minimizing the frequency of challenging the SR SSCs which in turn helps to keep the BDBEs beyond the design basis and preserve the design basis of the plant. The guideline also helps to maintain completeness in the selection of DBAs and in formulating the reliability and capability requirements for SR SSCs. The fact that many DBEs may have zero consequences does not justify avoidance of the other Table 5-2 guidelines or completion of the other DID evaluation components.

In a full application of the DID methodology, the DID evaluation would extend beyond the application of Table 5-2, which focus on plant capability for DID, and examine programmatic DID attributes and residual uncertainties surrounding the plant capability and programmatic actions in determining whether additional compensatory actions associated are useful. That full evaluation includes evaluating the completeness of the scenarios considered in generating the DBAs and selecting the SR SSCs; the LBE frequency and consequences margins; the available layers of defense associated with the prevention of initiating events; and the performance of SSCs that respond to the associated DBA. The IDP process questions should then strive to determining whether compensatory actions such as adding special treatment for non-safety-related SSCs are appropriate.

In the LMP methodology for SSC safety classification, SSCs in NSRST require that reliability and capability targets are set and a monitoring program is put in place to ensure those targets are met. That is the minimum special treatment for the NSRST category. Additional special treatments may or may not be selected as part of the DID IDP. However, the IDP considers the risk impacts of the SSCs in question, the risk impacts of any degradation of reliability and capability in setting the requirements as well as the meaningful benefits of taking any action. In the case where the DBE precursor to a DBA may not have any dose, if the resulting DBA does have offsite doses, additional performance confidence of precursor event SSC performance may be warranted. Likewise, special treatment of NST SSCs that could reduce the consequences of a risk-significant BDBE may be appropriate.

Question 2: If the DID adequacy evaluation for Layer 2 of Table 5-2 leads to special treatment on some SSCs in order to maintain DBEs with zero consequences below 10^{-2}, given the fact that such DBEs have zero risk, is it true that such SSCs are not safety significant?

Response

No. According to the LMP methodology, all SSCs that are classified as either SR or NSRST are classified as safety significant. Safety significant SSCs include those that perform risk-significant functions or functions that are necessary for adequate DID. In the case where the IDP decides to add some special treatment to a non-safety related SSC to maintain frequencies of DBEs in the DBE region, even if the affected DBEs have zero consequence, in order to meet the Layer 2 guidelines in Table 5-2 those SSC functions could be deemed necessary for adequate DID, and hence safety significant.

Question 3: Is there a large burden on the developer to have SSCs classified as NSRST?

Response

In the view of the LMP team, the use of a safety class such as NSRST on balance will yield burden reduction potential that will more than offset possible burden increases. The LMP safety classification approach was developed to be consistent with the safety significance definitions in 10 CFR 50.69 in which operating plants are utilizing risk insights to reduce programmatic burdens in operations. Establishing the NSRST category during design reduces the number of components assigned to the SR SSC category that will reduce manufacturing, construction, and operations burden on a larger set of SSCs. The minimum special treatment for NSRST is the need to set performance requirements for SSC reliability and capability in a monitoring program to assures those requirements are maintained. No additional treatments are necessary unless the IDP decides they are necessary.

Question 4: Does meeting guidelines in Table 5-2 automatically lead to adding SSCs to the NSRST category?

Response

No. Adding special treatment to a non-safety related SSC is just one option available to achieve DID adequacy. For instance, the full evaluation of DID adequacy involves the evaluation of layers of defense available for a sequence of LBEs in an event tree and the consequences,

including for LBEs in the BDBE region. Additionally, the margins and quantified LBE uncertainties should be considered when determining whether a risk-significant concern exists. The broader considerations included in the integrated decision process should be the final determinant of additional compensatory actions.

Example

To amplify on the above discussions, consider the example below, built on a generic event tree model used in the DID and SSC white papers to explain how SSCs contribute to the layers of defense and how SSC roles in preventing and mitigating LBEs are defined. Assume that a baseline assessment has been performed that resulted in an initial set of LBEs and SSC safety classifications. Part of this baseline assessment is associated with LBEs resulting from a specific initiating event, Plant Disturbance X as shown in Figure 1. The analysis of this initiating event yields 1 AOO, 1 DBE, and 1 BDBE. In the baseline assessment, it is assumed that the control system and SSC1 are classified as NST, and SSC2 is classified as SR SSC. The DBA associated with this DBE is described in Figure A-1.

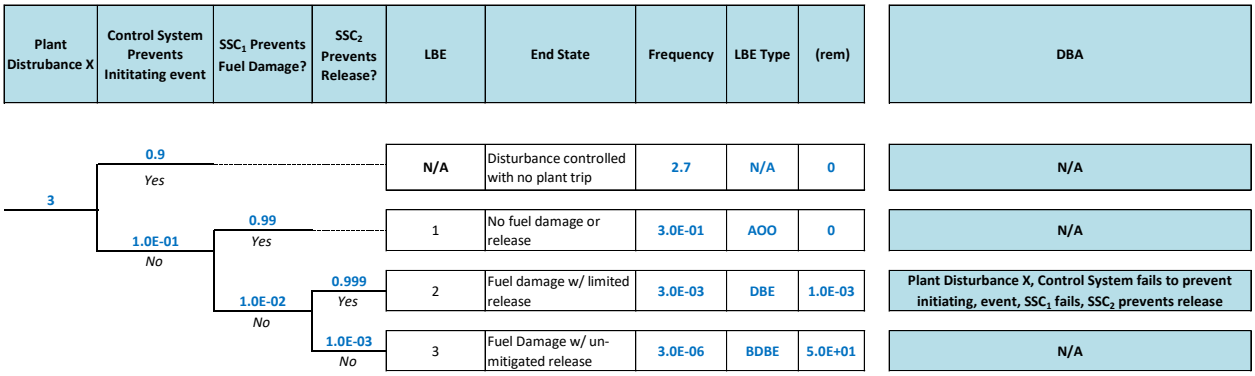


Figure A-1. Baseline Assessment for an Initiating Event: Plant Disturbance X

Note that the consequences assigned to the DBE are only 1 mrem, which is less than the 2.5-mrem dose significance threshold selected for evaluating LBE risks. For the purpose of making RIPB decisions in the LMP methodology, any doses less than 2.5 mrem are treated the same as those with zero consequence.

Then, at some later stage in the design process, there is an update that results in some changes to the reliability of plant systems. The changes in this update example are shown in Figure A-2.

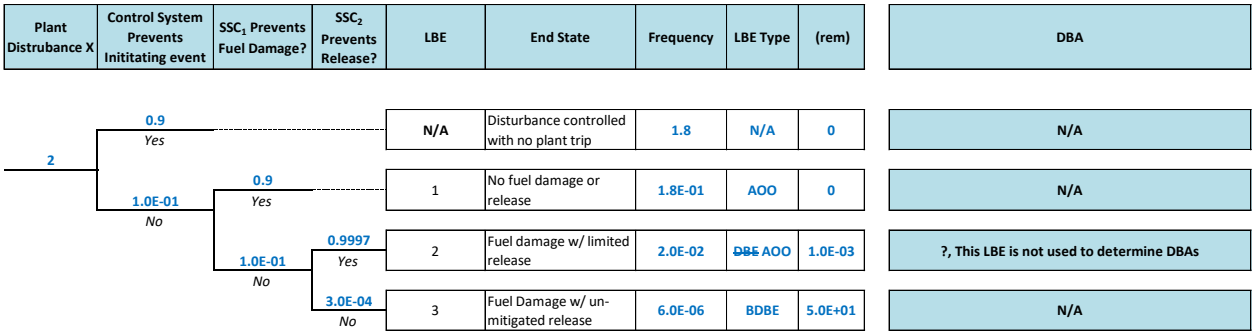


Figure A-2. Revised Assessment for Plant Disturbance X

As should be expected, the frequencies and failure probabilities are subject to change as the design evolves. In this example, it is noted that SSC1 has exhibited an order of magnitude increase in its failure probability whereas other changes reflect small improvements or remain the same. In this example, LBE 2 increases in frequency sufficiently to be reclassified as an AOO. This change is not keeping with the quantitative objective in Layer 2 of Table 2-2 of keeping DBEs less frequent than 10^{-2}/plant-year. In addition, the former DBE link to establishing the DBAs is no longer there.

One possible course of action in using the DID criterion is illustrated in Table A-1 below. This is just one possible course because there may be other steps that could be taken to get into alignment with the criterion such as steps to reduce the initiating event frequency which may be controlled by other SSCs not identified in this example. In this case, SSC1 would be reclassified as NSRST and the IDP could result in a reliability target of 10-2 to be in line with the baseline assessment and to help ensure there are sufficient special treatments such as performance monitoring to achieve and maintain this target. As seen in Table 1, steps taken to get improved reliability of SSC1 translate directly to improve the frequency of challenging the SR SSC from this initiating event. If the reliability target set by the IDP is maintained, the frequency of challenging the SR SSCs is maintained to the level in the baseline assessment.

Table A-1. Example Course of Action by IDP to Meet Layer 2 Quantitative Guideline

	Baseline Assessment		Revised Assessment	Application of DID Criteria
SSC	SSC Class	Failure Probability		
Control System	NST	1.0E-01	1.0E-01	remains NST
SSC_1	NST	1.0E-02	1.0E-01	Reclassify as NSRST, Set Reliability Target to 10^{-2}
SSC_2	SR SSC	1.0E-03	1.0E-03	remains SR
Frequency of Challenging SR SSC		3.0E-03	3.0E-02	SR SSC Challenge frequency controlled by SSC_1 target

This course of action would be followed up with another revised assessment that would reflect the steps to achieve improved reliability performance identified by the IDP.

In summary, the primary purpose of the DID adequacy criteria in Layer 2 of Table 2-2 is to control the frequency of challenging the SR SSCs. A secondary purpose is to maintain the completeness and robustness of the selection of DBAs, which is established by the selection of the DBEs.

APPENDIX B LMP DOCUMENTATION AND FREQUENTLY ASKED QUESTIONS

B.1 LMP Documentation

The LMP team prepared independent reports on each of the four major LMP elements. Additionally, the LMP team produced a narrative report describing the processes, events, and documents involved in producing the ultimate project deliverable product, NEI 18-04 "Risk-Informed Performance-Based Technology Inclusive Guidance for Non-Light Water Reactor Licensing Basis Development." Finally, the LMP team produced a report based on the experiences of early adopters of the LMP RIPB process which includes best practices, lessons learned, and frequently asked questions and responses. Table B-1 lists the Southern Company document numbers of each of these reports. The documents are available via the DOE's Office of Scientific and Technical Information (OSTI) public document repository (https://www.osti.gov).

Table B-1. LMP Reports and Document Numbers

Report Title	Southern Company Document Number	DOE OSTI Document Number
Selection and Evaluation of Licensing Basis Events	SC-29980-100 Rev 1	TBD
Probabilistic Risk Assessment Approach	SC-29980-101 Rev 1	TBD
Safety Classification and Performance Criteria for Structures, Systems, and Components	SC-29980-102 Rev 1	TBD
Risk-Informed and Performance-Based Evaluation of Defense-in-Depth Adequacy	SC-29980-103 Rev 1	TBD
Final Project Report	SC-29980-105 Rev. 1	TBD
LMP Lessons Learned, Best Practices, and Frequently Asked Questions	SC-29980-106 Rev 0	TBD

Licensing Basis Event Selection Approach

Inputs to the selection of LBEs are derived from a PRA of an advanced non-LWR plant. These inputs together with deterministic inputs, such as design selections and selection of Safety-Related (SR) 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 report, the engineering and safety analysis effort will result in a selection of a set of SR SSCs that are necessary and sufficient to perform the PRA Safety Functions (PSFs) 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 SR 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.

Probabilistic Risk Assessment Approach

This report outlines the approach to develop a PRA for advanced non-LWR plants in support of risk-informed and performance-based (RIPB) applications. Future advanced non-LWR license applications will include a design-specific PRA that is capable of supporting the applications for NRC permit(s) or license(s). When introduced at an early stage of the design, the PRA is expected to result in a more efficient risk management process. This report outlines the relevant regulatory policy and guidance for this type of PRA, describes the approach to be followed for the development of the PRA, and sets forth PRA topics that need to be addressed in order to facilitate successful design and more safety focused preparation and review of the license application.

SSC Safety Classification and Performance Requirements Approach

Information developed from and used in the development of the PRA to define event sequences and evaluate their frequencies and consequences is an input to the SSC safety classification and development of SSC performance targets. Information from the PRA is used to establish the necessary and sufficient conditions of SSC capability and reliability in order for LBE frequencies, consequences, and uncertainties to stay within the frequency-consequence evaluation criteria derived from the TLRC and to implement risk management strategies to control the total integrated risk of the plant. Reliability targets for SSCs are determined based on the need to maintain each LBE within its LBE category (Anticipated Operational Occurrence, Design Basis Event, or Beyond Design Basis Event). RIPB SSC capability targets are defined in part by the selected design margins between the LBE frequencies and dose limits for that LBE category. Special treatment requirements for SSCs are derived to achieve the necessary and sufficient degree of reliability and capability of the SSCs. This is discussed in a companion report on the LMP SSC safety classification approach.

Defense-in-Depth Adequacy

The PRA models and supporting assumptions are based in part on the plant capabilities for DID reflected in the design, as well as assumptions about the limits placed on design and operation of the plant by assumed programmatic DID measures. Information developed in the PRA is used to help evaluate the SSCs responsible for preventing and mitigating accidents. The PRA also plays an important role in the identification of key sources of uncertainty, and this supports a feedback loop to identify possible enhancements to plant capability and programmatic aspects of DID. Hence, the PRA provides important input to the risk-informed evaluation of DID, complements the NRC's deterministic approach and traditional DID philosophy, and provides a more objective, RIPB means to systematically demonstrate DID adequacy and preservation. This is discussed in a companion report on the LMP approach to evaluating DID adequacy.

LMP Final Report

The LMP team produced a narrative report describing the processes, events, and documents involved in producing the ultimate Project deliverable product, NEI 18-04 "Risk-Informed Performance-Based Technology Inclusive Guidance for Non-Light Water Reactor Licensing Basis Development." This report contains a wealth of references to documents that future users of the LMP RIPB process may find useful. Tables within the report provide references to the

NRC Agencywide Document Management System (ADAMS) Accession Numbers of many industry and NRC documents that future permit and license applicants may wish to reference in their own applications.

LMP Lessons Learned, Best Practices, and Frequently Asked Questions and Responses

The LMP team produced a report based on the experiences of early adopters of the LMP RIPB process which includes best practices, lessons learned, and frequently asked questions and responses. This report provides guidance to reactor designers on how to efficiently implement the LMP RIPB processes within their own organization and answers to 32 frequently asked questions from reactor designers.

B.2 Frequently Asked Questions

Probabilistic Risk Assessment Frequently Asked Questions

PRAQ1. How can the use of PRA technology to risk-inform the licensing of advanced non-LWRs be justified given the lack of operating experience with these reactors?

PRAQ2. How to develop adequate PRA data for initiating events and frequencies, component failure rates, maintenance unavailability, and other PRA data needs?

PRAQ3. What is the role of the PRA in the SSC safety classification process and how does safety classification influence the PRA models and data?

PRAQ4. What is the role of absolute and relative risk significance criteria in the LMP methodology?

PRAQ5. What is the applicability of 10 CFR 50 Appendix B to PRA in the LMP methodology?

PRAQ6. What is the available guidance for the systematic search for initiating events for the PRA on advanced non-LWRs?

PRAQ7. How does the LMP methodology identify and evaluate “cliff edge” effects?

PRAQ8. How does the structure of the PRA event tree logic impact the identification of the Required Safety Functions and the selection of the SR SSCs?

PRAQ9. How can the PRA standard requirements be met during the design stage when as-built and as-operated information is not available?

PRAQ10. What is the available guidance on how RSFs are determined, how they relate to FSFs?

PRAQ11. What guidance is available on the PRA treatment of safety functions provided via passive means and utilizing inherent reactor features?

PRAQ12. How can the LMP methodology be applied using dynamic PRA method?

PRAQ13. How does LMP address events that are not modeled in the PRA?

Licensing Basis Events Frequently Asked Questions

LBEQ1. What is the available guidance for how to develop mechanistic source terms using the PRA and supporting deterministic processes?

LBEQ2. How is the safety classification and special treatment of SSCs influenced by the placement of LBEs as AOOs vs. DBEs or BDBE?

LBEQ3. Is there additional information available on the selection of the F-C Target anchor points for evaluating the risk-significance of LBEs?

LBEQ4. What insights were obtained for using the F-C charts from the LMP tabletop exercises and from discussions with the NRC Staff regarding DG-1353 and SECY-19-0117?

SSC Classification Frequently Asked Questions

SSCQ1. What guidance is available on how to select among candidates for SR SSCs and possible conflicts with ARDCs?

SSCQ2. What guidance is available for how to classify NSRST SSCs and how to come up with STs.

SSCQ3. What guidance is available for how to consider whether an SSC is classified as NSRST as necessary for adequate DID?

SSCQ4. What guidance is available for how to address the full scope of SSCs in a plant including I&C, support systems, active SSCs, passive SSCs relying on inherent features, and SSCs necessary to implement safety significant operator actions?

SSCQ5. What guidance is available for how to consider the need to protect SR SSCs against DBEHLs and how to consider the requirements for NSR and NSRST SSCs?

SSCQ6. What guidance is available to discuss how SSC classification flows down from RSFs to major components and subcomponents to establish SRDC at the lowest level?

SSCQ7. What guidance is available on how to set reliability and capability targets for safety significant SSCs?

SSCQ8. What is the relationship between the Maintenance Rule scope and the LMP SSC approach to assuring reliability and capability targets for NSRST and NSR components?

SSCQ9. IEEE standards for I&C design only consider two safety classifications, 1E or non-1E. 1E is for safety functions or supporting systems that perform safety functions. Software QA for 1E is very complex and expensive. 1E V&V is also complex and difficult (i.e. exploration for unintended functions and behavior). The same concept of existing industrial codes and standards having binary rules for safety-related and non-safety-related SSC, but not addressing the

"middle" NSRST, is encountered often across standards development organizations. Should equipment classified by LMP as NSRST be treated as 1E or non-1E (or, as safety-related or non-safety-related) and why?

Defense-in-Depth Frequently Asked Questions

DIDQ1. What guidance is available on how to examine the results, limitations, uncertainties, and omissions from the PRA for making IDP decisions that impact SSC safety classification and ST or deciding on practical compensatory actions?

DIDQ2. What guidance is available on how to organize the IDP and update the DID baseline through design iterations?

DIDQ3. What is the distinction between the IDP and the IDPP and why is it important?

DIDQ4. What additional guidance is there regarding the evaluation of Plant Capability DID for low dose or no dose (zero consequences) LBEs and the determination of NSRST SSCs?

Project Management Frequently Asked Questions

PMQ1. What guidance is available for how to manage the iterative process of design development, PRA development, and selection of codes and standards for SSCs?

PMQ2. How does a designer know that they are completely done implementing the LMP RIPB process with a reactor design? What is the definitive "pencils down" "finish line" event?