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

Risk-Informed Performance-Based Guidance for Non-Light Water Reactor Licensing Basis Development

WORKING DRAFT

Draft Report Revision M

Document Number
SC-29980-xx Rev M

May 27, 2018

Disclaimer

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

Prologue

This guidance document represents a framework for the efficient licensing of advanced non-light water reactors (non-LWRs). It is the result of a Licensing Modernization Project (LMP) led by Southern Company and cost-shared by the U.S. Department of Energy (DOE). The LMP prepared this document for establishing licensing technical requirements to facilitate risk-informed and performance-based design and licensing of advanced non-LWRs. Such a framework acknowledges enhancements in safety achievable with advanced designs and reflects current states of knowledge regarding safety and design innovation, creating an opportunity for reduced regulatory complexity with increased levels of safety.

Abstract

This guideline 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-light water reactors. This guidance provides an acceptable means for addressing the aforementioned topics as part of demonstrating a specific design provides reasonable assurance of adequate radiological protection.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

AOO	Anticipated Operational Occurrence
ATWS	anticipated transient without scram
BDBE*	Beyond Design Basis Event
CDF	core damage frequency
CFR	Code of Federal Regulations
DBA	Design Basis Accident
DBE*	Design Basis Event
DID	defense-in-depth
EAB	Exclusion Area Boundary
EPA	Environmental Protection Agency
F-C	Frequency-Consequence
FDC	Functional Design Criteria
FMEA	failure modes and effects analysis
GDC	General Design Criteria
HAZOP	hazard and operability study
HPB	helium pressure boundary
HTGR	high temperature gas-cooled reactor
HTS	Heat Transport System
IAEA	International Atomic Energy Agency
IDP	Integrated Decision Panel
IE	Initiating Event
ISI	In-service inspection
LBE*	Licensing Basis Event
LERF	large early release frequency
LMP	Licensing Modernization Project
LRF	large release frequency
LWR	light water reactor
MHTGR	a specific prismatic modular high-temperature gas-cooled reactor developed by the Department of Energy
NEI	Nuclear Energy Institute
NRC	Nuclear Regulatory Commission
NSRST*	Non-Safety-Related with Special Treatment
NST*	Non-Safety-Related with No Special Treatment
O&M	Operations and Maintenance
PAG	Protective Action Guide
PBMR	Pebble Bed Modular Reactor
PHA	process hazard analysis
PRA	probabilistic risk assessment
PRISM	Power Reactor Innovative Small Module
QA	Quality Assurance
QHO	Quantitative Health Objective
RCCS	Reactor Cavity Cooling System
RCS	Reactivity Control System
RIDM	risk-informed integrated decision-making
RIM	Reliability and Integrity Management
RIPB	risk-informed and performance-based
RIPB-DM	risk-informed and performance-based integrated decision-making
SAP	Safety Assessment Principle
SBO	station blackout
SCS	Shutdown Cooling System
SR*	Safety-Related
SRP	Standard Review Plan
SSC	structures, systems, and components
TI-RIPB*	technology-inclusive, risk-informed, and performance-based
TLRC*	Top Level Regulatory Criteria

*These terms have special meanings defined in this document.

1.0 INTRODUCTION

1.1 Purpose

This document presents a technology-inclusive, risk-informed, 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-light water reactors including but not limited to molten salt reactors, high temperature gas cooled reactors, and a variety of fast reactors at all thermal power capacities. This guidance provides applicants a potentially acceptable method for establishing the aforementioned topics as part of demonstrating a specific design provides reasonable assurance of adequate radiological protection.

1.2 Background

The Nuclear Regulatory Commission (NRC) communicated their expectations for advanced reactors in the 2008 NRC Policy Statement on the Regulation of Advanced Reactors, [73 FR 60612; ADAMS ML082750370],

> *"...the Commission expects that advanced reactors will provide enhanced margins of safety and/or use simplified, inherent, passive, or other innovative means to accomplish their safety and security functions."*

The advanced non-light water reactor (non-LWR) developers are proposing new and innovative designs which promise to meet these Commission expectations. The NRC intends to achieve its mission through adhering to the principles of good regulation—independence, openness, efficiency, clarity, and reliability. The NRC Staff noted in the report "Near-Term Task Force Review of Insights from the Fukushima Dai-ichi Accident" that the current nuclear regulatory infrastructure,

> *"...was developed for the purpose of reactor licensing in the 1960s and 1970s and supplemented as necessary to address significant events or new issues."*

To modernize the regulation, in 1995 the Commission published their Final Policy Statement on the Use of Probabilistic Risk Assessment Methods in Nuclear Regulatory Activities [60 FR 42622; ADAMS ML021980535] which states in part,

> *"The use of PRA technology should be increased in all regulatory matters to the extent supported by the state-of-the art in PRA methods and data and in a manner that complements the NRC's deterministic approach and supports the NRC's traditional defense-in-depth philosophy."*

This document builds on these landmark policy statements by providing a foundation upon which a more fully risk-informed performance-based technical licensing environment can be developed while allowing the current regulatory framework to be used by the early movers.

1.3 Applicability and Scope

This document describes acceptable processes for selection of LBEs; safety classification of SSCs and associated risk-informed special treatments; and determination of DID adequacy applicable to a technology-inclusive array of advanced non-light water reactor designs. The scope of this document is focused on establishing guidance for advanced (i.e., non-LWR) designs so license applicants can develop inputs that can be used to comply with applicable regulatory requirements, including but not limited to the following:

- 10 CFR 50.34(a) describes the content required in the Preliminary Safety Analysis Report (PSAR) for a Construction Permit application.
- 10 CFR 50.34(b) describes the content required in the Final Safety Analysis Report (FSAR) for an Operating License application.
- 10 CFR 52.47 describes the required information for a FSAR associated with a Standard Design Certification application.
- 10 CFR 52.79 describes the required information for a FSAR associated with a Combined License application.
- 10 CFR 52.137 describes the required information for a FSAR associated with a Standard Design Approval application.
- 10 CFR 52.157 describes the required information for a FSAR associated with a Manufacturing License application.

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

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

Background discussions of each of these topics, including examples, may be found in the four documents submitted to the NRC in the course of development of this guidance document

[*] In this document, licensing basis events are defined in terms of event sequences comprised of an initiating event, the plant response to the initiating event which includes a sequence of successes and failures of mitigating systems, and a well-defined end state. The term event sequence is used in lieu of the term accident sequence used in LWR PRA standards because the scope of the LBEs includes AOOs and initiating events with no adverse impacts on public safety. The only use of the term accident in the LMP process is with the term "Design Basis Accident" which is one of the LBE categories developed for Chapter 15 of the safety analysis report. It is recognized that some design and licensing requirements (e.g. definition of the safe shutdown earthquake) are defined for individual events rather than event sequences.

content: Defense-in-Depth Adequacy [ML17354B174], Licensing Basis Event Selection [ML17104A254], Probabilistic Risk Assessment [ML17158B543], and Structures, Systems, and Components Safety Classification [ML17290A463].

2.0 LICENSING BASIS DEVELOPMENT PROCESS

The overall objective of this guidance document is to describe a systematic and reproducible framework for selection of LBEs, classification of SSCs, and determination of DID adequacy such that different knowledgeable parties would come to like conclusions. These assessments are key to the development of applications for licenses, certifications or approvals because they provide necessary insights into the scope and level of detail for the description of plant SSCs and programmatic controls in the application. This framework facilitates a systematic iterative process for completion of tasks as the design progresses, providing immediate feedback to the designer to make better informed decisions.

This section includes descriptions of the following TI-RIPB processes:

- Systematic definition, categorization, and evaluation of event sequences for selection of licensing basis events (LBEs), which include Anticipated Operational Occurrences (AOOs), Design Basis Events (DBEs), Design Basis Accidents (DBAs), and Beyond Design Basis Events (BDBEs).
- Systematic safety classification of SSCs, development of performance requirements, and application of special treatments.
- Guidelines for evaluation of DID adequacy.

These processes are:

- Risk-informed to fully utilize the insights from the systematic risk assessment in combination with structured prescriptive rules to address the uncertainties which are not addressed in the risk assessment. This approach will provide reasonable assurance that adequate protection is provided for public radiological protection.
- Performance-based to evaluate effectiveness relative to realizing desired outcomes that is achieved by using quantifiable performance metrics for LBE frequencies and consequences, and performance requirements for SSC capabilities to prevent and mitigate accidents. This is an alternative to a prescriptive approach specifying particular features, actions, or programmatic elements to be included in the design or process as the means for achieving desired objectives.

The processes in this guidance document can be used to:

- Develop simplified, yet logical, coherent, and complete bases for the development of the safety design approach; and, evaluation of the safety design approach based on the specific technology and design.
- Apply a sound probabilistic risk assessment (PRA), including appropriate probabilistic models based on available standards, to develop and evaluate the safety design approach for a design.

In summary, the outcomes from executing the processes include design specific physical features (i.e., SSCs), actions, or programmatic elements that give the NRC adequate assurance that:

- The selected LBEs adequately cover the range of hazards that a specific design is exposed to and reflect the impacts of SSC failure modes that are appropriate for the design.
- The LBEs are defined in terms of successes and failures of SSCs that perform safety functions. Safety functions are defined as those functions responsible for the prevention and mitigation of an unplanned radiological release from any source within the plant.
- The SSCs that perform the safety functions are adequately capable, reliable, diverse, and redundant across the layers of defense in the design.
- The philosophy of DID is apparent in the design and programmatic features included in the licensing application and outcomes of systematic evaluations of DID adequacy
- Sufficient and integrated design decisions are made, trading off plant capabilities and programmatic capabilities based on risk-informed insights with respect to providing reasonable assurance of adequate protection.
- The scope and level of detail for plant SSCs and programmatic controls included in applications are commensurate with their safety and risk significance.

The processes covered in this guidance document are integrated and highly interdependent, starting with the process for the LBEs selection. The SSC classification process ensures that the SSCs that are considered to be risk significant based on their contribution to the credited prevention or mitigation functions, or are considered to be important DID contributors, have adequate reliability and availability. A mitigation function of an SSC is one in which successful implementation of the function along an event sequences helps to limit the consequences of the event sequence. A prevention function of an SSC is one in which the reliability of the SSC contributes to reducing the frequency of a more adverse event sequence. This guidance document is organized as follows for the implementation process:

- Section 3.0 provides a description of the LBE selection and evaluation process.
- Section 4.0 provides a description of SSC classification and derivation of performance requirements.
- Section 5.0 provides a description of the DID adequacy determination.

3.0 SELECTION OF LICENSING BASIS EVENTS

3.1 Licensing Basis Event Definitions

NRC regulatory requirements for a reactor design refer to several different kinds of events included within the licensing basis including AOOs, DBEs, postulated accidents, design basis accidents (DBAs), and BDBEs. The guidance document definitions in Table 3-1 are intended to establish transparent and consistent quantification of existing terms without changing their intent or expected use.

Table 3-1. Definitions of Licensing Basis Events

Event Type	Current Definition or Common Use	Guidance Document Definition
Anticipated Operational Occurrences (AOOs)	*"Conditions of normal operation that are expected to occur one or more times during the life of the nuclear power unit and include but are not limited to loss of power to all recirculation pumps, tripping of the turbine generator set, isolation of the main condenser, and loss of all offsite power."*[*] [SRP 15.0 and 10 CFR 50 Appendix A]	Event sequences expected to occur one or more times during the life of the nuclear power plant, which may include one or more reactor modules. Events and event sequences with 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.
Design Basis Events (DBEs)	*"Conditions of normal operation, including AOOs, design-basis accidents, external events, and natural phenomena, for which the plant must be designed to ensure functions of safety-related electric equipment that ensures the integrity of the reactor coolant pressure boundary; the capability to shut down the reactor and maintain it in a safe shutdown condition; or the capability to prevent or mitigate the consequences of accidents that could result in potential offsite exposures."* [SRP 15.0]	Event sequences that are expected to occur one or more times in the life of an entire fleet of nuclear power plants, but are less likely than an AOO. Events and event sequences with 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 to form the design basis of the plant is the same as in the NRC definition. However, DBEs do not include normal operation and AOOs as defined in the NRC references.
Beyond Design Basis Events (BDBEs)	"*This term is used as a technical way to discuss accident sequences that are possible but were not fully considered in the design process because they were judged to be too unlikely. (In that sense, they are considered beyond the scope of design-basis accidents that a nuclear facility must be designed and built to withstand.) As the regulatory process strives to be as thorough as possible, 'beyond design-basis' accident sequences are analyzed to fully understand the capability of a design."* [NRC Glossary]	Event sequences that are not expected to occur in the life of an entire fleet of nuclear power plants. Events and 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. The objective of BDBEs to assure the capability of the plant is the same as in the NRC definition.
Design Basis Accidents (DBA)	*"Postulated accidents that are used to set design criteria and limits for the design and sizing of safety-related systems and components."* [SRP 15.0] "*A postulated accident that a nuclear facility must be designed and built to withstand without loss to the systems, structures, and components necessary to ensure public health and safety*." [NRC Glossary and NUREG-2122]	Postulated accidents that are used to set design criteria and performance objectives for the design and sizing of SSCs that are classified as safety-related. 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 SSCs classified as safety-related are available to mitigate postulated accident consequences to within the 10 CFR 50.34 dose limits.
Licensing Basis Events (LBEs)	Term not used formally in NRC documents.	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 normal operation, AOOs, DBEs, BDBEs, and DBAs.

[*] SRP 15.0 further breaks down AOOs into events with "moderate" frequency (i.e., events expected to occur several times during the plant life) and "infrequent" (i.e., events that may occur during the plant life).

For normal operations, including AOOs, the NRC regulations are, for the most part, generic and can be applied to an advanced non-LWR plant. The applicant is required to classify the events considered within the design basis as either AOO or Design-Basis Accident (DBA) based on a list of historically considered events for LWRs and with subjective assessment of the expected frequency of occurrence. For advanced non-LWRs, the supplied lists of generic LWR events is not adequate and a subjective frequency assignment has limited applicability to non-LWR designs. Therefore, the following systematic and reproducible process is provided to derive the appropriate list of LBEs as one acceptable process to assist with meeting the requirements.

3.2 Advanced Non-LWR LBE Selection Approach

3.2.1 TLRC Frequency–Consequence Evaluation Criteria

Based on insights from the review of existing regulatory criteria, this approach uses a set of frequency–consequence criteria; this frequency–consequence evaluation correlation, hereafter referred to as the F-C Target, is shown in Figure 3-1.

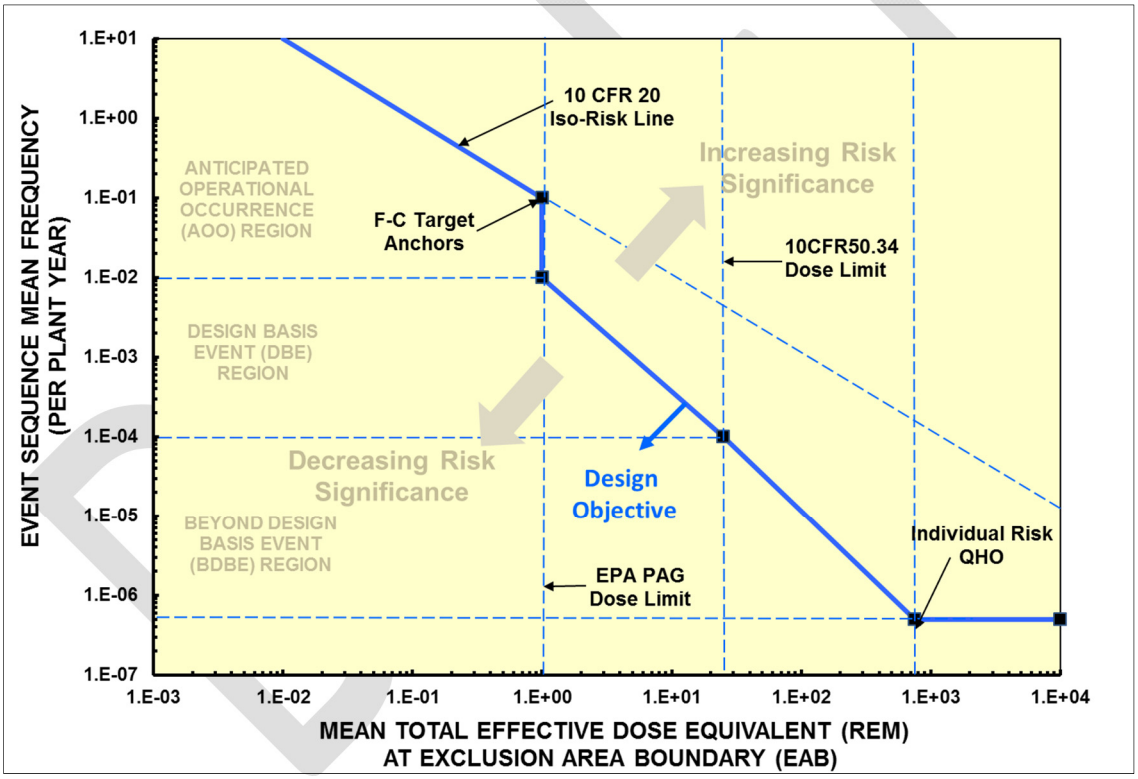

Figure 3-1. Frequency-Consequence Target

The F-C Target in this figure is based on the following considerations:

- LBE categories are based on mean event sequence frequency of occurrence per plant-year. AOOs are off-normal events that are expected to occur in the life of the plant with frequencies exceeding 10^{-2} per plant-year, where a plant may be comprised of multiple reactor modules. DBEs are less frequent events that may be expected to occur in the

lifetime of a fleet of plants with frequencies between 10^{-4} to 10^{-2} per plant-year. BDBEs are rare events with frequencies less than 10^{-4}/plant-year but with upper bound frequencies greater than 5×10^{-7}/plant-year. LBEs may or may not involve release of radioactive material and may involve two or more reactor modules or radionuclide sources.

- The regions of the graph separated by the frequency-dose evaluation line are identified as "Increasing Risk" and "Decreasing Risk" to emphasize that the purpose of criteria is to evaluate the risk significance of individual LBEs and to recognize that risk evaluations are not performed on a pass-fail basis in contrast with deterministic safety evaluation criteria. This change is consistent with NRC risk-informed policies such as those expressed in RG 1.174 in which risk insights are used along with other factors within an integrated decision-making process.
- The target values shown in the figure should not be considered as a demarcation of acceptable and unacceptable results. The targets provide a general reference to assess events, SSCs, and programmatic controls in terms of sensitivities and available margins.
- The evaluation line doses for high frequency AOOs down to a frequency of 10^{-1}/plant-year are based on an iso-risk profile defined by the annual exposure limits of 10 CFR 20, i.e. 100 mrem/plant-year.
- The doses for AOOs at frequencies of 10^{-1}/plant-year down to 10^{-2}/plant-year are set at a reference value of 1 rem corresponding with the Environmental Protection Agency (EPA) Protective Action Guide (PAG) limits and consistent with SRP Chapter 15.0 acceptance criteria for lower frequency AOOs for PWRs. It is expected that many LBEs will not release any radioactive material and the identification of plant capabilities to prevent such releases is a factor considered in the formulation of SSC safety classification and performance requirements as discussed more fully in the section below on SSC safety classification. The F-C Target for DBEs range from 1 rem at 10^{-2}/plant-year to 25 rem at 10^{-4}/plant-year. This aligns the lowest frequency DBEs to the limits in 10 CFR 50.34 and provides continuity to the lower end of the AOO criteria. A straight line on the log-log plot connects these criteria.
- The F-C Target for the BDBEs range from 25 rem at 10^{-4}/plant-year to 750 rem at 5×10^{-7}/plant year to ensure that the Quantitative Health Objective (QHO) for early health effects is not exceeded for individual BDBEs. The question of meeting the QHOs for the integrated risks over all the LBEs is addressed using separate cumulative risk targets described later in this guidance document.
- The frequency-dose anchor points used to define the shape of the curve are indicated in the figure. The lines between the anchor points are straight lines on a log frequency vs. log dose graph.
- In consideration of the risk aversion principle, the logarithmic slope of the curve in the DBE and BDBE regions exceeds -1.5 which corresponds to the most conservative limit-line proposed by Farmer to address risk aversion.
- The F-C Target used in Figure 3-1 provides the basis for establishing the risk significance of LBEs. The EPA PAG dose guidance value for a specified distance (e.g. the exclusion area boundary) may be overlaid against the F-C Target to define more ambitious target for

those designs intending to establish alternative requirements of offsite emergency planning zones. However, the F-C Target in Figure 3-1 is still used to determine LBE and SSC risk significance.

Across the entire spectrum of the F-C chart, the F-C Target is selected such that the risk defined as the product of the frequency and consequence does not increase as the frequency decreases. In addition, the principle of risk aversion (reduced risk target as consequences increase) is applied at frequencies below 10^{-2}/plant-year.

While interpreting the 10 CFR 20 annual exposure limits of 100 mrem/year, it is recognized that the use of this criteria in developing the F-C Target is to be applied to individual LBEs. To establish an aggregate risk measure including AOOs and other lower consequence events, the LBE process includes an activity to assure that the total frequency of exceeding 100 mrem summed over all the LBEs do not exceed 1/year. This limit serves to control the risks in the high frequency low consequence end of the event spectrum noting that the NRC Safety Goal QHO cumulative risk targets are most effective in controlling the low frequency, high consequence end of the spectrum. The LBE approach includes performance of an integrated assessment over all the LBEs to ensure that NRC safety goal QHOs for both early and latent health effects are met.

3.2.2 LBE Selection Process

A flow chart indicating the steps in identifying and evaluating LBEs in concert with the design evolution is shown in Figure 3-2. These steps are carried out by the design and design evaluation teams responsible for establishing the key elements of the safety design approach and preparing a license application. The process can be used to prepare an appropriate licensing document, e.g., licensing topical report, that describes the derivation of the LBEs. The LBE selection and evaluation process is implemented in LBE selection tasks described below.

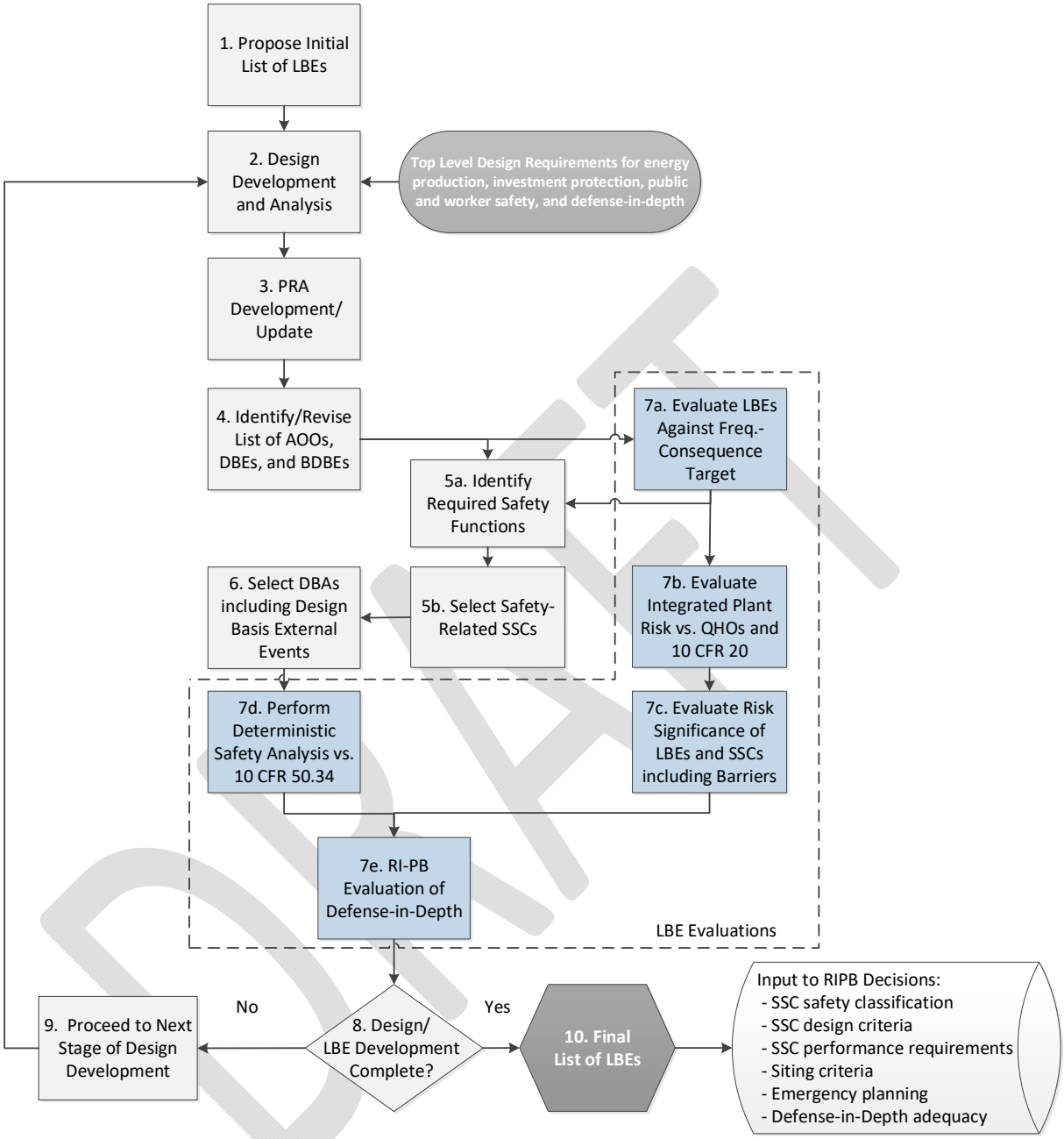

Figure 3-2. Process for Selecting and Evaluating Licensing Basis Events

Task 1: Propose Initial List of LBEs

During design development, it is necessary to select an initial set of LBEs which may not be complete but are necessary to develop the basic elements of the safety design approach. These events are to be selected deterministically based on all relevant and available experience including prior experience from the design and licensing of reactors. The initial selection of events can also be supported by analysis techniques such as engineering judgment, FMEAs, and HAZOPs. In many cases, the designer may also have an initial assessment regarding which SSCs will be classified as safety-related to meet the safety design approach for the reactor design. This

classification would also be deterministically based using the same information utilized for the initial selection of LBEs.

Task 2: Design Development and Analysis

The design development is performed in phases and often includes a pre-conceptual, conceptual, preliminary, and final design phase and may include iterations within phases. The design development and analysis includes definition of the key elements of the safety design approach, the design approach to meet the top level design requirements for energy production and investment protection, and analyses to develop sufficient understanding to perform a PRA and the deterministic safety analyses. The subsequent Tasks 3 through 10 may be repeated for each design phase or iteration until the list of LBEs becomes stable and is finalized. Because the selection of deterministic DBAs requires the selection of safety-related SSCs, this process also yields the selection of safety-related SSCs that will be needed for the deterministic safety analysis in Task 7d. The sequence of design phases would be somewhat different if the LBEs are being used to support a Design Certification Application or a Combined Operating License.

Task 3: PRA Development/Update

A PRA model is developed and then updated as appropriate for each phase of the design. Prior to first introduction of the PRA, it is necessary to develop a technically sound understanding of the potential failure modes of the reactor concept, how the reactor plant would respond to such failure modes, and how protective strategies will be incorporated into formulating the safety design approach. The incorporation of safety analysis methods appropriate to early stages of design, such as failure modes and effects analysis (FMEA) and process hazard analysis (PHA), provide early stage evaluations that are systematic, reproducible and as complete as the current stage of design permits. As described in Section 3.3, developers are encouraged to begin developing the PRA early to support all design phases. However, developers have flexibility regarding when to introduce and develop the PRA to improve upon the initial risk management approaches or intentionally conservative analyses and related design features. If undertaken the early design phases, the PRA is of limited scope, coarse level of detail, and makes use of engineering judgment much more than a completed PRA that would meet applicable PRA standards. The scope and level of detail of the PRA are then enhanced as the design matures and siting information (or site envelope) is defined. For modular reactor designs, the event sequences modeled in the PRA would include event sequences involving a single or multiple reactor modules or radionuclide sources. This approach provides useful risk insights to the design to ensure that accident sequences involving multiple reactor modules are not risk significant. The PRA process exposes sources of uncertainty encountered in the assessment of risk and provides estimates of the frequencies and doses for each LBE including a quantification of the impacts of uncertainties using quantitative uncertainty analyses and supported by sensitivity analyses.

Task 4: Identify/Revise List of AOOs, DBEs, and BDBEs

The event sequences modeled and evaluated in the PRA are grouped into accident families each having a similar initiating event, challenge to the plant safety functions, plant response, end state, and mechanistic source term if there is a radiological release. Each of these families is assigned to an LBE category based on mean event sequence frequency of occurrence per plant-year

summed over all the event sequences in the LBE family. The event families from this step may confirm or revise the initial events identified in Task 1.

AOOs are off-normal events that are expected to occur in the life of the plant with frequencies exceeding 10^{-2} per plant-year, where a plant may be comprised of multiple reactor modules. DBEs are less frequent events that may be expected to occur in the lifetime of a fleet of plants with frequencies between 10^{-4} to 10^{-2} per plant-year. BDBEs are rare events with frequencies less than 10^{-4}/plant-year but with upper bound frequencies greater than 5×10^{-7}/plant-year. LBEs may or may not involve release of radioactive material and may involve two or more reactor modules or radionuclide sources. For LBEs with no radiological release, it is important to identify challenges to SSCs, including barriers that are responsible for preventing or mitigating a release of radioactive material.

Event sequences with upper 95th percentile frequencies less than 5×10^{-7}/plant-year are retained in the PRA results and used to confirm there are no cliff-edge effects. They are also taken into account in the RIPB evaluation of defense-in-depth in Task 7e.

Note: Tasks 5a, 5b, and 6 should be performed together in parallel rather than sequentially.

Task 5a: Identify Required Safety Functions

In Task 5a the full set of DBEs are examined to identify the safety functions that are necessary and sufficient to meet the F-C Target for all DBEs and high consequence BDBEs, and to conservatively ensure that 10 CFR 50.34 dose requirements can be met. High consequence BDBEs are those with consequences that exceed 10 CFR 50.34 dose criteria. For the DBEs these safety functions, when fulfilled are responsible for mitigating the consequences within the F-C target. Required safety functions for any high consequence BDBEs are responsible for preventing them from increasing in frequency into the DBE region and outside the F-C target by exhibiting sufficient reliability performance to keep the BDBE frequency sufficiently low.

Task 5b: Select/Revise Safety-Related SSCs

For each of these required safety functions identified in Task 5a, a decision is made on which SSCs that perform these required safety functions and are found to be available on all the DBEs should be classified as safety related. Structures and physical barriers that are required to protect any safety-related SSCs in performing their required safety functions in response to any design basis external event are also classified as safety-related. Safety-related SSCs are also selected for any required safety function associated with any high consequence BDBEs in which the reliability of the SSC is required to keep the event in the BDBE frequency region. The remaining SSCs that are not classified as safety-related are considered in other evaluation tasks including Tasks 7b, 7c, 7d, and 7e. Performance targets and design criteria for both safety-related and non-safety-related SSCs are developed and described more fully in SSC white paper Section 4.0 - SSC Safety Classification.

Task 6: Select Deterministic DBAs and Design Basis External Events

For each DBE identified in Task 4, a deterministic DBA is defined that includes the required safety function challenges represented in the DBE, but assumes that the required safety functions are performed exclusively by safety-related SSCs and all non-safety SSCs that perform these same functions are assumed to be unavailable. These DBAs are then used in Chapter 15 of the

license application for supporting the conservative deterministic safety analysis. NRC Regulatory Guide 1.203, "Transient and Accident Analysis Methods," provides additional discussion of developing appropriate evaluation models for analyzing DBAs.

DBEs initiated by an external event would be used to help define requirements to protect safety-related SSCs from such events. When supported by available methods, data, design and site information, and available PRA guides and standards, external events reflected in the LBEs will be derived from the PRA. In other cases not supported by the PRA, e.g. external flooding at river sites, design basis external initiating events may be selected using traditional methods common to existing reactors.

Some design basis external events such as a design basis external flood or design basis seismic event may impact multiple modules concurrently, however a design objective would be to prevent a substantial[*] release for such events. To achieve these design objectives, there should be no risk significant DBEs involving a release from two or more modules, and any BDBEs that involve releases from multiple reactor modules or sources would not be high consequence BDBEs. When this objective is achieved, there should be no DBAs with significant releases from two or more modules or radionuclide sources.

Task 7: Perform LBE Evaluations

The deterministic and probabilistic safety evaluations that are performed for the full set of LBEs are covered in the following five tasks.

Task 7a: Evaluate LBEs Against F-C Target

In this task the results of the PRA which have been organized into LBEs will be evaluated against a F-C Target as shown in Figure 3-1. The figure does not define specific acceptance criteria for the analysis of LBEs but rather a tool to focus the attention of the designer and those reviewing the design and related operational programs to the most significant events and possible means to address those events. The NRC's Advanced Reactor Policy Statement includes expectations that advanced reactors will provide enhanced margins of safety. The safety margin between the design-specific PRA results and the F-C Target provides one useful and practical demonstration of how the design fulfills the Commission expectations for enhanced safety. These margins also are useful in the evaluation of defense-in-depth adequacy in Step 7d. The evaluations performed in this task are done for each LBE separately. The mean values of the frequencies are used to classify the LBEs into AOOs, DBEs, and BDBE categories. However, when the uncertainty bands[†] defined by the 5th percentile and 95th percentile of the frequency estimates straddles a frequency boundary, the LBE is evaluated in both LBE categories. An LBE with mean frequency above 10^{-2}/plant-year and 5th percentile less than 10^{-2}/plant-year is evaluated as an AOO and DBE. An LBE with mean frequency less than 10^{-4}/plant-year with a 95th percentile above 10^{-4}/plant-year is evaluated as a BDBE and a DBE. Uncertainties about the

[*] The term substantial is used to mean that the site boundary dose when combined with the LBE frequency would not result in a risk significant LBE.

[†] It is recognized that the PRA may not fully resolve the impacts of all sources of uncertainty, such as modeling uncertainty. The LMP approach to PRA recommends following the guidance in NUREG-1855 to address uncertainties. Uncertainties not quantified in the PRA are important inputs to the evaluation of defense-in-depth adequacy in Task 7e.

mean values are used to help evaluate the results against the frequency-consequence criteria and to identify the margins against the criteria.

DBE doses are evaluated against the F-C Target based on the mean estimates of consequence[*]. This approach is based on the fact that the use of a conservative dose evaluation is appropriate for the deterministic safety analysis in Task 7a but is not consistent with the way in which uncertainties are addressed in risk-informed decision making in general, where mean estimates supported by a robust uncertainty analysis are generally used to support risk significance determinations. When evaluating risk significance, comparing risks against safety goal QHOs, evaluating changes in risk against the Regulatory Guide 1.174 change in risk criteria, the accepted practice has been to first perform a quantitative uncertainty analysis and then to use the mean values to compare against the various goals and criteria, which are set in the context of uncertainties in the risk assessments.

The primary purpose of comparing the frequencies and consequences of LBEs against the F-C Target is to evaluate the risk significance of individual LBEs. The objective for this approach is that uncertainties in the risk assessments are evaluated and included in discussions of design features and operational programs related to the most significant events and possible measures to address those events. The evaluations in this task are based on mean frequencies and mean doses for all three LBE categories. One exception to this is that BDBEs with large uncertainties in their frequencies are evaluated as DBEs when the upper 95th percentile of the frequency exceeds 10^{-4} per plant-year; and AOOs with lower 5th percentile frequencies below 10^{-4}/plant year are also evaluated as DBEs. The uncertainties about these means are considered as part of the RIPB DID evaluation in Task 7e.

Part of the LBE frequency-dose evaluation is to ensure that LBEs involving radiological releases from two or more reactor modules do not make a significant contribution to risk and to ensure that measures to manage the risks of multi-module or multi-source accidents are taken[†].

The final element of the LBE evaluation in this step is to identify design features that are responsible for keeping the LBEs within the F-C Target including those design features that are responsible for preventing or mitigating risk-significant releases for those LBEs with this potential. This evaluation leads to performance requirements and design criteria that are developed within the framework of the SSC classification step in the risk-informed, performance based approach.

Task 7b: Evaluate Integrated Plant Risk against QHOs and 10 CFR 20

In this task, the integrated risk of the entire plant including all the LBEs is evaluated against three cumulative risk targets including:

[*] If the developer choses to use a conservative, deterministic approaches (e.g., MHA) in lieu of RIPB approaches, other means will need to be developed to establish safety classification, risk significance, safety significance and DID adequacy as described in this guidance.

[†] The term "plant" is used to define the entity that is being subjected to the LMP process for LBE selection and evaluation and may be comprised of a single reactor or multiple reactor modules. In addition, the plant is expected to include additional non-reactor sources of radioactive material. Hence each LBE may involve one or more reactor modules or radionuclide sources.

- The total frequency of exceeding a site boundary dose of 100 mrem from all LBEs shall not exceed 1/plant-year. This metric is introduced to ensure that the consequences from the entire range of LBEs from higher frequency, lower consequences to lower frequency, higher consequences are considered. The value of 100 millirem is selected from the annual exposure limits in 10 CFR 20.
- The average individual risk of early fatality within 1 mile of the Exclusion Area Boundary (EAB) from all LBEs shall not exceed 5×10^{-7}/plant-year to ensure that the NRC Safety Goal QHO for early fatality risk is met.
- The average individual risk of latent cancer fatalities within 10 miles of the EAB from all LBEs shall not exceed 2×10^{-6}/plant-year to ensure that the NRC safety goal QHO for latent cancer fatality risk is met.

One element of this step is to identify design features that are responsible for preventing and mitigating radiological releases and for meeting the integrated risk criteria. This evaluation leads to performance requirements and design criteria that are developed within the framework of the SSC classification step in the guidance document.

In addition to the two QHOs, the 10 CFR 20 criterion is considered in recognition that the referenced regulatory requirement is for the combined exposures from all releases even though it has been used in developing the F-C Target used for evaluating the risks from individual LBEs. Having these cumulative risk targets as part of the process provides a mechanism to ensure that the F-C Target is conservatively defined for use as a tool for focusing attention on matters important to managing the risks from non-LWRs.

Task 7c: Evaluate Risk Significance of LBEs and SSCs Including Barriers

In this task, the details of the definition and quantification of each of the LBEs in Task 7a and the integrated risk evaluations of Task 7b are used to define both the absolute and relative risk significance of individual LBEs and SSCs which include radionuclide barriers. These evaluations include the use of PRA risk importance metrics, where applicable, and the examination of the effectiveness of each of the layers of defense in retaining radionuclides. LBEs are classified as risk significant if the LBE site boundary dose exceeds a small fraction of background radiation exposure and the frequency of the dose is within 1% of the F-C Target. SSCs are classified as risk significant if the SSC function is required to keep any LBEs inside the F-C Target, or if the total frequency of LBEs with the SSC failed is within 1% of any of the three cumulative risk targets identified in Step 7b. This information is used to provide risk insights, to identify safety significant SSCs, and to support the RIPB evaluation of defense-in-depth in Task 7e.

Task 7d: Perform Deterministic Safety Analyses Against 10 CFR 50.34

This task corresponds to the traditional deterministic safety analysis that is found in Chapter 15 of the license application. It is performed using conservative assumptions. The uncertainty analyses in the mechanistic source terms and radiological doses that are part of the PRA are available to inform the conservative assumptions used in this analysis and to avoid the arbitrary "stacking" of conservative assumptions.

Task 7e: Risk-Informed, Performance-Based Evaluation of Defense-in-Depth

In this task, the definition and evaluation of LBEs will be used to support a RIPB evaluation of defense-in-depth. This task involves the identification of key sources of uncertainty, and evaluation against defense-in-depth criteria. Outcomes of this task include possible changes to the design to enhance the plant capabilities for defense-in-depth, formulation of conservative assumptions for the deterministic safety analysis, and input to defining and enhancing programmatic elements of defense-in-depth.

It is noted that this DID evaluation does not change the selection of LBEs directly. This evaluation could lead to compensatory actions that change the design capability or programmatic controls on the design, which in turn would lead to changes in the PRA and thereby affect the selection or evaluation of LBEs.

This may be a convenient point for designers to assess plant features for effective compliance with regulatory requirements such as 10 CFR 50.155, "Mitigation of Beyond-Design Basis Events," and 10 CFR 73, "Physical Protection of Plants and Materials." The results from the evaluation will also support related licensing matters such as defining appropriate constraints in terms of siting (10 CFR 100), offsite emergency planning, and development of plant procedures and guidelines.

Task 8: Decide on Completion of Design/LBE Development

The purpose of this task is to decide if additional design development is needed, either to proceed to the next logical stage of design or to incorporate feedback from the LBE evaluation that design, operational, or programmatic improvements should be considered. Such design improvements could be motivated by a desire to increase margins against the frequency-consequence criteria, reduce uncertainties in the LBE frequencies or consequences, manage the risks of multi-unit accidents, limit the need for restrictions on siting or emergency planning, or enhance the performance against defense-in-depth criteria. The DID adequacy evaluation may result in additional need to iterate on the adequacy of design, operational, and programmatic programs, which in turn could influence the PRA and result in a need for cycling through all the LBE evaluation steps.

Task 9: Proceed to Next Stage of Design Development

The decision to proceed to the next stage of design is reflected in this task.

Task 10: Finalize List of LBEs and Safety-Related SSCs

Establishing the final list of LBEs and safety-related SSCs signifies the completion of the LBE selection process and the selection of the safety-related SSCs. The next step in implementing the TI-RIPB approach is to complete the SSC safety classification process and to formulate performance requirements and design criteria for SSCs that are necessary to control the LBE frequencies and doses and other performance standards associated with the protection of fission product barriers. Important information from Task 7a through 7e is used for this purpose.

3.2.2.1 Evolution of LBEs Through Design and Licensing Stages

The LBE selection flow chart in Figure 3-2 reflects an iterative process involving design development, PRA development, selection of LBEs, and evaluation of LBEs. The process flow

chart can be viewed as beginning in the pre-conceptual or conceptual design phase when many design details are unavailable, the PRA effort has not begun, and the safety design approach is just being formulated. To begin the process outlined in Figure 3-2, an initial set of LBEs is proposed based on engineering judgment in Task 1 of the process. This may generate an initial target selection of safety-related SSCs.

During the conceptual design phase, different design concepts are explored and alternatives are considered to arrive at a feasible set of alternatives for the plant design. The effort to develop a PRA should begin during this phase. Traditional design and analysis techniques are applied during conceptual design, including (1) use of traditional design bases of engineering analysis and judgment, (2) application of research and development programs, (3) use of past design and operational experience, (4) performance of design trade studies, and (5) decisions on how or whether to conform to established applicable LWR-based reactor design criteria and whether other principle criteria are needed.

Creation of the initial event list of LBEs includes expert evaluation and review of the relevant experience gained from previous reactor designs and associated PRAs, when available. It starts by answering the first question in the risk triplet series: "What can go wrong?"; "How likely is it?"; and "What are the consequences?" Care must be exercised to ensure that information taken from other reactor technologies is interpreted correctly for the reactor technology in question. The body of relevant reactor design and PRA data that is available to draw upon may vary for different reactor technologies. Once design alternatives and trade studies are developed, the safety design approach can be defined. A review of the major systems can take place and techniques such as a failure modes and effects analysis (FMEA) and process hazards analyses such as hazard and operability studies (HAZOPs) can be applied to identify initial failure scenarios and to support the initial PRA tasks to define initiating events.

Preliminary design activities need to balance regulatory and design requirements, cost, schedule, and other owner requirements to optimize the design, cost, and capabilities that satisfy the objectives for the reactor facility.

As the design matures, the scope and level of detail of the PRA is expanded and is used to help support design decisions along the way. An early simplified PRA can be very helpful to support design trade studies that may be performed to better define the safety design approach. Questions that arise in the efforts to build a PRA model may be helpful to the design team especially in the mutual understanding of what kind of challenges will need to be addressed. Because the design is being changed more frequently at this point and better characterized as the design phases evolve, the PRA results and their inputs to the LBE selection process will also be subject to change. As a result, refinements to the list of LBEs are expected. The simplifying perception that a design has stages that contain bright lines is a frequent description at the system level but is not correct at the plant level. Different parts of the design mature at different times. Systems often go through design stages like this, however, at any moment, there may be systems in many design phases simultaneously. Consequently, the PRA development is a continuum as well, maturing with the systems design. PRA updates with system development then provide a more frequent, integrated plant performance check that is otherwise missing in the conventional design process and will also provide risk insights to help the design decisions. When the design, construction, and PRA are developed in a manner that is sufficient to meet PRA requirements

reflected in applicable PRA standards and regulatory guides, the LBEs will be finalized and included in the license application.

3.3 Role of the PRA in LBE Selection

Applicants under the 10 CFR 52 framework are required by NRC regulations to develop a PRA (10 CFR 50.71(h)) and to provide a description of the results of the PRA in their application (e.g., 10 CFR 52.79). While 10 CFR 50 Construction Permit or Operating License applications do not currently require a PRA, the development and use of the PRA during the design process can be more efficient than completing the design and then developing the PRA. The primary motivation to utilize inputs from a PRA in the selection of LBEs is that it is the only method available that has the capability to identify the events that are specific and unique to a new reactor design. Traditional methods for selecting LBEs, such as those reflected in the General Design Criteria and Chapter 15 of the Standard Review Plan, do not refer to a systematic method for identifying design specific events. The generic lists of events provided in the SRP guidance as examples for transients and postulated accidents to consider are specific to LWRs. Traditional systems analysis techniques that can be used to evaluate a design and were used to define the LBEs for currently licensed reactors, including FMEAs, HAZOPs, single failure analyses, etc., have been incorporated into the PRA methodology for selecting initiating events and developing event sequence models. PRA is also a mature technology that is supported by industry consensus standards and regulatory guides. There are no similar consensus standards for deterministic selection of LBEs for new reactor designs. Although much of the available experience in PRA has been with operating LWR plants, there is a rich history of PRA as applied to advanced non-LWR designs including HTGRs, the British MAGNOX and AGR gas-cooled reactors, and liquid metal-cooled fast reactors. A trial use PRA standard for advanced non-LWRs was issued by the ASME/ANS Joint Committee on Nuclear Risk Management in 2013. The trial use PRA standard has been subjected to a number of PRA pilot studies on the Power Reactor Innovative Small Module (PRISM), HTR-PM project in China, and several other non-LWR designs. Lessons from these pilot studies are being incorporated into the revised non-LWR PRA standard.

Prior to first introduction of the design-specific PRA, it is necessary to develop a technically sound understanding of the potential failure modes of the reactor concept, how the reactor plant would respond to such failure modes, and how protective strategies will be incorporated into formulating the safety design approach. The incorporation of safety analysis methods appropriate to early stages of design, such as FMEA and PHA, provide industry-standardized practices to ensure that such early stage evaluations are systematic, reproducible and as complete as the current stage of design permits.

The interfaces between traditional systems engineering processes and the initial development of the PRA model are shown in Figure 3-3. It is important to note that the systems engineering inputs on the left hand side of the diagram are fundamental to developing the design. However, with the concurrent development of the PRA model, the PRA is developed in parallel with the design and thereby is available to provide important risk insights to the design development and supporting systems analyses. Decisions to defer the introduction of the PRA to later stages of the design process lead to reduced opportunities for cost-effective risk management.

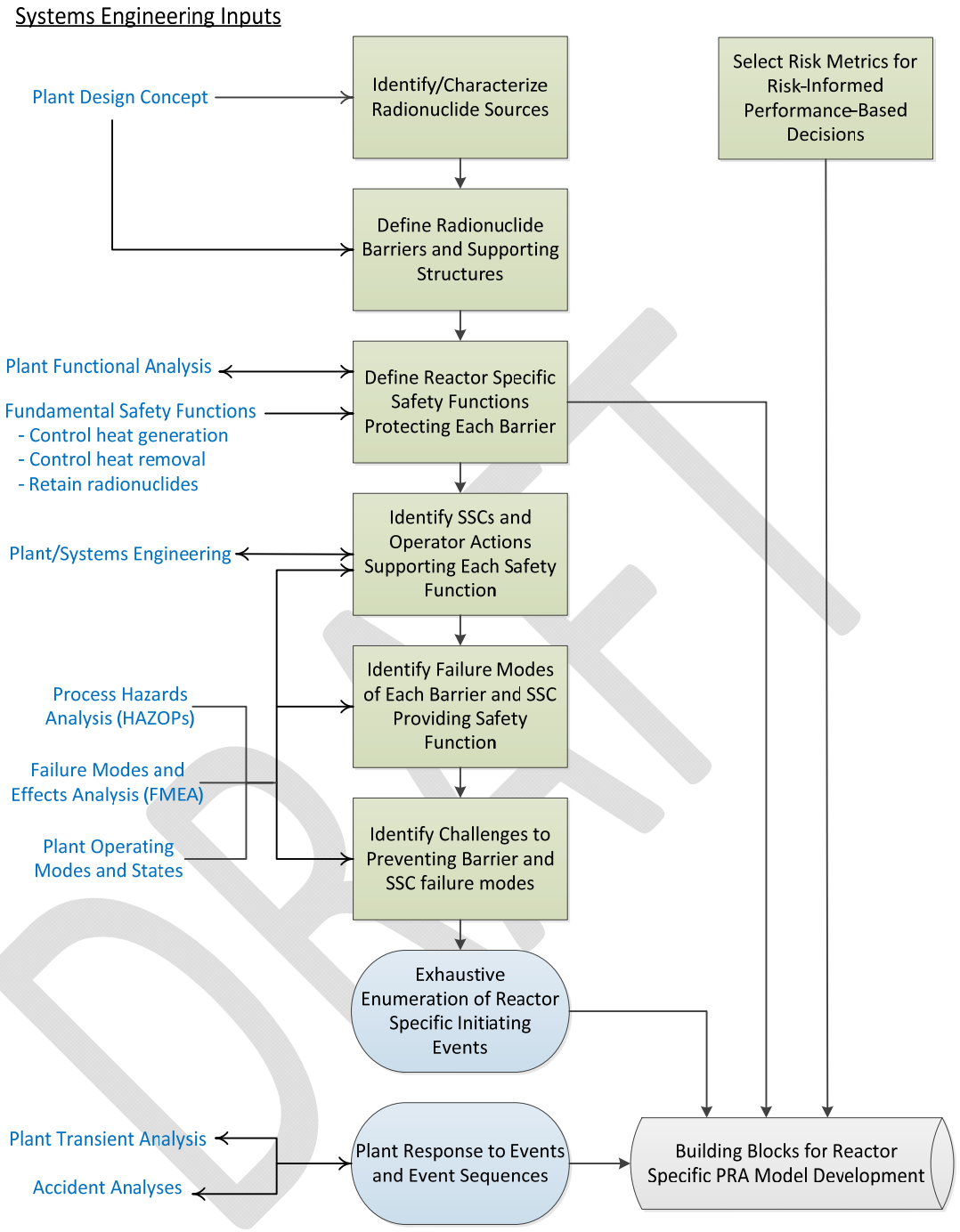

Figure 3-3. Flow Chart for Initial PRA Model Development

The PRA will be used to evaluate the safety characteristics of the design and to provide a structured framework from which the initial set of LBEs will be risk-informed. The evaluation of the risks of the LBEs against the frequency–consequence correlation helps make the LBE selection process both risk-informed and performance-based. This evaluation framework is critical to the development of a revised licensing framework. It highlights the issues that deserve the greatest attention in a safety-focused process. Subsequently the PRA will provide important input to the formulation of performance targets for the capability and reliability of the SSCs to

prevent and mitigate accidents and thereby contribute to the performance- based aspects of the design and licensing development process. In addition, engineering judgment and utilization of relevant experience will continue to be used to ensure that LBE selection and classification is complete. The PRA will systematically enumerate event sequences and assess the frequency and consequence of each event sequence. Event sequences will include internal events, internal plant hazards, and external events. The modeled event sequences will include the contributions from common cause failures and thereby will not arbitrarily exclude sequences that exceed the single failure criterion.

Each event sequence family reflected in the LBE definitions is defined as a collection of event sequences that similarly challenge plant safety functions. This means that the initiating events within the family have a similar impact on the plant such that the event sequence development following the plant response will be the same for each sequence within the family. If the event sequence involves a radiological release, each sequence in the family will have the same or similar mechanistic source term and offsite radiological consequences. Many of the LBEs do not involve a release and understanding the plant capabilities to prevent release is an extremely important insight back to the design. Event sequence family grouping facilitates selection of LBEs from many individual events into a manageable number.

The PRA's quantification of both frequencies and consequences will address uncertainties, especially those associated with the potential occurrence of rare events. The quantification of frequencies and consequences of event sequences, and the associated quantification of uncertainties, provides an objective means of comparing the likelihood and consequence of different scenarios against the F-C correlation. The scope of the PRA, when completed, should cover a full set of internal and external events and determination of radiological consequences when the design is completed and site characteristics are defined. Designers may propose to address all or parts of the process by assessing fission product barriers and showing that radioactive materials are retained within the facility with a high degree of confidence. Such an approach would still require that some of the information provided by a PRA, including the identification of challenges to the barriers and identification and evaluation of dependencies among the barriers.

The PRA will include event sequences involving two or more reactor modules, if applicable, as well as two or more sources of radioactive material. This will enable the identification and evaluation of risk management strategies to ensure that sequences involving multiple modules and sources are not risk significant. The NRC staff has developed technical criteria for evaluating multi-module risk. These technical criteria would ensure that multi-module plants are designed and operated in such a way to demonstrate that the accident sequences are not significant contributors to risk and large release events, and, if these events should occur, to mitigate their impact on the public health and safety. Additionally, these criteria ensure that relevant risk insights related to multi-module design and operation are captured and well understood by the staff, applicants, and the public.

The LBE selection process is not risk-based, but rather risk-informed as there are strong deterministic inputs to the process. First, the PRA development is anchored to traditional deterministic system engineering analyses that involve numerous applications of engineering judgment, as identified in the left side of Figure 3-3. These include FMEAs, process hazards

assessment, application of relevant experience from design and licensing of other reactors, and deterministic models of the plant response to events and accidents. Second, the deterministic DBAs are selected based on prescriptive rules and analyzed using conservative assumptions. Finally, the LBE selection includes a review to ensure that the LBE selection and the results of the LBE evaluations meet a set of guidelines to evaluate the adequacy of defense-in-depth.

These evaluations often lead to changes to the plant design and programmatic controls that are reflected in changes to the PRA and, hence, changes to the selection of LBEs and SSC safety classification. In addition to these elements, peer reviews and regulatory reviews of the PRA will provide an opportunity to challenge the completeness and treatment of uncertainties in the PRA to ensure that the deterministic DBAs and the conservative assumptions that are used in Chapter 15 are sufficient to meet the applicable regulatory requirements.

3.3.1 Use of PRA in LBE Selection Process Summary

In the course of developing a reactor design-specific PRA model, a comprehensive set of initiating events and event sequence families are systematically identified, building on the engineering and systems analyses that are performed to support the design development. These events and event sequences are considered in the selection of the LBEs, and the quantitative estimates of the event sequence frequencies and consequences provide a basis for evaluating their risk significance. Deterministic evaluations of prescriptively derived DBAs benefit from the identification and evaluation of LBE uncertainties that result from the PRA process.

SSC safety classification requires an assessment of the risk significance of SSCs and the LBEs that describe the safety functions of the SSCs in the prevention and mitigation of accidents. Information from the PRA is used as input to the selection of reliability targets and performance requirements for SSCs that set the stage for the selection of special treatment requirements.

The PRA process, in the course of addressing the three questions of the risk triplet: “What can go wrong?”, “How likely is it?”, and “What are the consequences?”, exposes many sources of uncertainty in the definition of event sequences, the estimation of their frequencies, and the quantification of the consequences. This information on uncertainties is an important input to the selection of protective strategies and in the evaluation of defense-in-depth adequacy. Additional roles of the PRA in the DID evaluation include information on the LBE risk margins against the F-C Target and the Cumulative Risk Targets, and evaluation of quantitative DID evaluation criteria.

The above uses of the PRA complement the use of deterministic methods traditionally employed in the development of the design and licensing bases as part of risk-informed, rather than risk-based framework.

3.3.2 Non-LWR PRA Scope for LBE Selection

Prior to the first use of the PRA, it is necessary to develop an understanding of the potential failure modes of the reactor concept, how the reactor plant would respond to such failure modes, and how protective strategies are incorporated into formulating the safety design approach. The incorporation of safety analysis methods appropriate to early stages of design, such as failure

modes and effects analysis (FMEA), HAZOPs, and other process hazard analysis (PHA) methods, provide industry-standardized and established practices to ensure that early stage evaluations are systematic, reproducible and as complete as the current stage of design permits.

Since the non-LWRs are expected to make greater use of inherent and passive capabilities to achieve safety, the PRA model used for applications described in this document should address the full spectrum of internal events and external hazards that pose challenges to the capabilities of the plant.

The size, complexity, and potential risk of a given design should influence the level of detail required to support this process. Reactor designs with small radionuclide inventories, few SSC, and inherently safe responses to upsets may employ simple, yet fit for purpose, PRAs.

Quantification of the frequencies and radiological consequences of each of the significant event sequences modeled is an important outcome of the PRA. This quantification includes mean point estimates and an appropriate quantification of uncertainty in the form of uncertainty probability distributions. These distributions should account for quantifiable sources of parameter and model uncertainty in the accident frequencies, mechanistic source terms, and offsite radiological consequences. The analysis performed in support of the RIPB applications covered in this guideline should include an appropriate set of sensitivity analyses to provide adequate assurance that major contributors to risk and performance uncertainties are identified and addressed.

Plants comprised of multiple reactor modules require consideration of event sequences that impact reactor modules independently as well as those that impact two or more reactor modules concurrently.

3.3.3 PRA Scope Adequacy

For non-LWRs, the guidance in the ASME/ANS RA-S-1.4 provides an acceptable means to establish the scope and technical adequacy of the PRA.

The scope and level of detail of the PRA models aligns with the state of definition of the design, the safety design approach, and systems design concepts. As the design matures and more design information becomes available for different types of risk evaluations, the scope of the PRA can broadened to address other plant conditions and progressively confirm the plant capability to meet safety objectives.

Given the simple systems, inherent characteristics, and minimal possible public health hazard expected of many non-LWR designs, especially those with low power levels, the PRA complexity required to support decision-making and an application should be much less complex than for operating LWR plants. Designers should note that 10 CFR 50.47 and 10 CFR 52.79 require 10 CFR 52 applications to address frequency and consequences of events from AOOs to Postulated Accidents regardless of reactor size or design for which some aspects of PRA may be needed.

3.3.4 PRA Safety Functions

The term "PRA safety function" as used in the LMP is any function by any SSC modeled in the PRA that is responsible for preventing or mitigating a release of radioactive material from any radioactive material source within the plant. Some of these safety functions should be further classified as "required safety functions" if they are necessary to ensure that all the DBEs have doses that fall within the F-C Target and also to ensure that the doses for the DBAs meet the requirements of 10 CFR 50.34 using conservative assumptions. Once those required safety functions are defined, SSCs that are available to support those functions on all the DBEs are identified. In addition, SSCs whose reliability needs to be assured to prevent any high consequence BDBEs from migrating up into the DBE region are also identified. From these sets of SSCs, the designer selects a set of safety related SSCs to perform each required safety function.

Safety functions are defined starting with generic fundamental reactor functions of controlling heat generation, controlling heat removal, and retaining radionuclides. These are refined as necessary into reactor technology-specific safety functions that reflect the reactor concept and unique characteristics of the reactors. This provides the foundation for reactor technology specific SSCs selected to perform each function.

3.3.5 Selection of Risk Metrics for PRA Model Development

3.3.5.1 Overall Plant Risk Metrics

The PRA model can be structured differently than the model for an LWR PRA, given that plant damage states may not involve an equivalent metric to the core damage state in a LWR PRA model. Frequencies of event sequences can be individually identified and grouped into accident families having the same or similar plant response and offsite radiological consequences may be defined in terms of plant response, mechanistic source term, and offsite radionuclide consequences. Consequences are quantified in terms of offsite early and latent health effects and/or site boundary doses.

Some acceptable TI-RIPB risk metrics include:

- Integrated risks of a given consequence metric, e.g., site boundary dose, number of early or latent health effects, etc. calculated by summing the product of the frequency and consequence of each LBE over the full set of LBEs.
- Integrated risks of individual fatalities as needed for comparison to the Cumulative Risk Targets for evaluating LBEs including the QHOs.
- Cumulative frequency of exceeding consequences such as large radiological release, early or latent health effects, or a specific site boundary dose.

In addition to the above TI metrics, reactor specific risk metrics defined by the owner may be used to define the parameters of the PRA model. Requirements for the definition and use of these reactor specific metrics are given in the Advanced non-LWR PRA Standard.

The selection of PRA risk metrics should address event sequences that may involve one or more reactor modules or non-reactor radionuclide sources. This is addressed using the following approaches:

- The IEs and event sequences in the PRA delineate events involving each reactor and radionuclide source separately as well as events involving two or more reactors or sources.
- Dependencies associated with shared systems and structures are explicitly modeled in an integrated fashion to support an integrated risk assessment of the entire plant where the plant may be comprised of two or more reactor modules and non-core radionuclide sources.
- Treatment of human actions considers the unique performance shaping factors associated with multi-reactor and multi-source event sequences.
- Treatment of common cause failures delineates those that may impact multiple reactor modules.
- The frequency basis of the event sequence quantification is events per (multi-module/multi-source) plant-year.

3.3.5.2 Risk Significance Evaluations

There are two types of risk significance evaluations that are performed for the selection and evaluation of LBEs. The first type is an evaluation of the frequencies and consequence of each LBE, expressed in the form of mean values and uncertainty (at the 5^{th} and 95^{th} percentiles), against the Frequency-Consequence (F-C) Target. In this evaluation, the frequencies and consequences of individual LBEs are compared against an F-C Target derived from top level regulatory requirements and NRC safety goal policy. The objective is to keep the LBE frequencies and consequences within the F-C Targets. An evaluation of the margins between the LBE risks and the F-C Target is one aspect of the RIPB evaluation of plant capability and defense-in-depth adequacy. The development of the F-C Target is explained more fully in the LBE white paper.

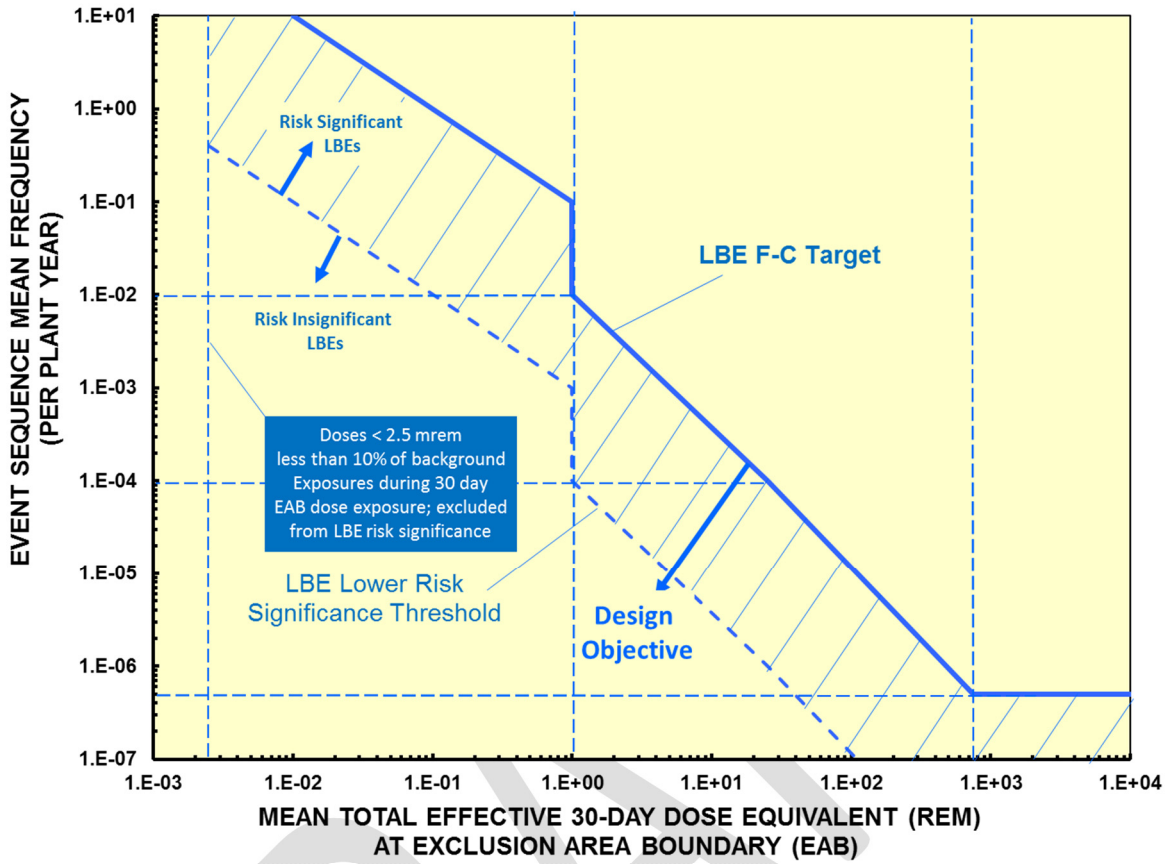

Figure 3-4. Use of the F-C Target to Define Risk Significant LBEs

Each LBE in this evaluation is defined as a family of event sequences modeled in the PRA that groups the individual modeled PRA event sequences according to the similarity of the following elements of the event sequence:

- Plant operating state at the time of the initiating event.
- Initiating Events (IE).
- Plant response to the IE and any independent or consequential failures represented in the event sequence, including the nature of the challenge to the barriers and SSCs supporting each safety function.
- Event sequence end state.
- Combination of reactor modules and radionuclide sources affected by the sequence.
- Mechanistic source term (MST) for sequences involving a radiological release.

The event sequence frequencies are expressed in terms of events/plant-year where a plant may be comprised of two or more reactor modules and sources of radioactive material.

In addition to evaluation of each individual LBE, an integrated risk evaluation of the entire plant is performed against the below criteria. For this evaluation, the integrated risk of the entire plant is evaluated against three Cumulative Risk Targets:

- The total frequency of exceeding a site boundary dose of 100 mrem from all LBEs shall not exceed 1/plant-year. This metric is introduced to ensure that the consequences from the entire range of LBEs from higher frequency, lower consequences to lower frequency, higher consequences are considered. The value of 100 millirem is selected from the annual exposure limits in 10 CFR 20.
- The average individual risk of early fatality within 1 mile of the EAB shall not exceed 5×10^{-7}/plant-year to ensure that the NRC Safety Goal QHO for early fatality risk is met.
- The average individual risk of latent cancer fatalities within 10 miles of the EAB shall not exceed 2×10^{-6}/plant-year to ensure that the NRC safety goal QHO for latent cancer fatality risk is met.

Risk significant LBEs are those with frequencies and consequences within 1% of the F-C Target with site boundary doses exceeding 2.5 mrem. To consider the effects of uncertainties, the upper 95th percentile estimates of both frequency and dose should be used. The use of the 1% metric is consistent with the approach to defining risk significant accident sequences in the PRA standards. The 2.5 mrem cut-off is selected as this is approximately 10% of the dose that an average person at the site boundary would receive in 30 days due to background radiation.

To provide input to the selection of emergency planning zones, the frequency of exceeding the Environmental Protection Agency protective action guideline dose limits would be included in the calculated risk metrics.

3.3.6 Contributors to Risk and Risk Importance Measures

To derive useful risk insights from the results of a PRA, it is necessary to understand the principal contributors to each evaluated risk metric. This can be achieved by rank ordering the PRA event sequences and sequence minimal cut-sets to identify their relative and absolute contribution to each risk metric and to calculate the risk importance measures that evaluate contributions to basic events that may be common to two or more sequences or cut-sets. For any of the integrated risk metrics, such as the QHOs, the relative risk significance of any LBE can be calculated as a percentage of the LBE risk (product of the LBE frequency and LBE consequence) to the aggregated risk of all the LBEs.

In order to evaluate the risk contributions from basic events that may appear in two or more event sequences or cut-sets, risk importance measures can be used. The most commonly used risk importance measures in PRA are listed in Table 3-2. In this table, the term R represents the total risk, $R(base)$, which is the risk with each basic event probability set to its base value, and the term x_i represents the probability of a basic event i, which may be, for example, the event that a specific valve fails to perform its function.

Measure	Abbreviation	Principle
Risk reduction	RR	$R(\text{base}) - R(x_i = 0)$
Fussell–Vesely	FV	$\frac{R(\text{base}) - R(x_i = 0)}{R(\text{base})}$
Risk reduction worth	RRW	$\frac{R(\text{base})}{R(x_i = 0)}$
Criticality importance	CR	$\frac{R(x_i = 1) - R(x_i = 0)}{R(\text{base})} \times x_i(\text{base})$
Risk achievement	RA	$R(x_i = 1) - R(\text{base})$
Risk achievement worth	RAW	$\frac{R(x_i = 1)}{R(\text{base})}$
Partial derivative	PD	$\frac{R(x_i + \partial x_i) - R(x_i)}{\partial x_i}$
Birnbaum importance	BI	$R(x_i = 1) - R(x_i = 0)$

Table 3-2. Risk Importance Measures

The associated Table 3-1 risk importance measures definitions can be used with any of the technology-inclusive risk metrics selected for the PRA using this process. These include:

- Frequency of a specific LBE
- Total risk (sum of the product of frequency and site boundary dose) of all the PRA modeled sequences, or individual risk of fatality in the plant vicinity
- Frequency of exceeding a specified site boundary dose
- Individual risk of prompt or latent fatality for comparison to NRC safety goal QHOs.

The historical approach to evaluating risk importance produced only the relative importance of each basic event because the formulas are normalized against the total calculated risk for the plant, *R(base)*. For advanced non-LWR plants, the frequencies of accidents involving a release of radioactive material may be very small and those accidents with releases may involve very small source terms compared with releases from an LWR core damage accident. Hence, it is appropriate to evaluate risk significance not only on a relative but also on an absolute basis.

For this purpose, the risks can be compared against the risk goals rather than the baseline risks. One example of the use of absolute risk metrics is the approach to defining risk significance LBEs as illustrated in Figure 3-1. Another metric is used in establishing the risk significance of SSCs. For this metric, SSCs are risk significant if any of the following criteria are met:

- A prevention or mitigation function of the SSC is necessary to meet the design objective of keeping all LBEs within the F-C Target. This is determined by assuming failure of the SSC in performing a prevention or mitigation function and checking how the resulting LBE risks compare with the F-C Target. The LBE is considered within the F-C Target

when a point defined by the upper 95th percentile uncertainty of the LBE frequency and dose estimates is within the F-C Target.

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

[*] This evaluation of SSC risk significance requires the aggregation of all the LBEs in which any basic event in the PRA model associated with the SSC is failed. There are normally different basic events for different SSC failure modes (e.g. failure to start, failure to run, etc.), unavailability for test or maintenance, or a common cause basic event involving that SSC. When the total frequency of LBEs with all the basic events associated with the SSC exceeds the 1% criterion, the SSC is regarded as risk significant according to these criteria.

4.0 SAFETY CLASSIFICATION AND PERFORMANCE CRITERIA FOR STRUCTURES, SYSTEMS, AND COMPONENTS

The purpose of this section is to define the approach to SSC safety classification and to identify potential technical concerns related to SSC safety classification and the derivation of requirements necessary to support SSC performance of safety functions in the prevention and mitigation of LBEs. Such requirements include those to provide the necessary capabilities to perform their mitigation functions and those to meet their reliability requirements to prevent LBEs with more severe consequences. Use is made of relevant aspects of risk-informed SSC classification approaches that have been developed for existing and advanced LWRs and small modular reactors, including those defined for implementation of 10 CFR 50.69.

Safety classification categories are defined as follows:

- Safety-Related (SR):
    - SSCs selected by the designer from the SSCs that are available to perform the required safety functions to mitigate the consequences of DBEs to within the LBE F-C Target, and to mitigate DBAs that only rely on the SR SSCs to meet the dose limits of 10 CFR 50.34 using conservative assumptions
    - SSCs selected by the designer and relied on to perform required safety functions to prevent the frequency of BDBE with consequences greater than the 10 CFR 50.34 dose limits from increasing into the DBE region and beyond the F-C Target
- Non-Safety-Related with Special Treatment (NSRST):
    - Non-safety-related SSCs relied on to perform risk significant functions. Risk significant SSCs are those that perform functions that prevent or mitigate any LBE from exceeding the F-C Target, or make significant contributions to the cumulative risk metrics selected for evaluating the total risk from all analyzed LBEs.
    - Non-safety-related SSCs relied on to perform functions requiring special treatment for DID adequacy
- Non-Safety-Related with No Special Treatment (NST):
    - All other SSCs (with no special treatment required)

Safety significant SSCs include all those SSCs classified as SR or NSRST. None of the NST SSCs are classified as safety significant.

It is noted that some SSCs classified as NST may have requirements to ensure that SSC failures following a design basis internal or external event does not adversely impact SR or NSRST SSCs in their performance of safety significant functions.

The RIPB SSC performance and special treatment requirements identified in this process for SR and NSRST SSCs are complimentary activities. The purpose of these requirements is to provide reasonable confidence in the SSC capabilities and reliabilities in performing functions identified in the LBEs consistent with the F-C Target and the regulatory dose limits for DBAs.

4.1 SSC Safety Classification Approach for Advanced Non-LWRs

The SSC safety classification* process is described in Figure 4-1. This process is designed to be used with the process for selecting and evaluating LBEs. The information needed to support the SSC safety classification is available when Step 10 of the LBE selection and evaluation process is completed in each phase of the design process.

* The SSC safety classification process classifies SSCs on the basis of the SSC safety functions reflected in the LBEs. Although the SSCs are classified, the resulting performance and special treatment requirements are for the specific functions identified in the LBEs.

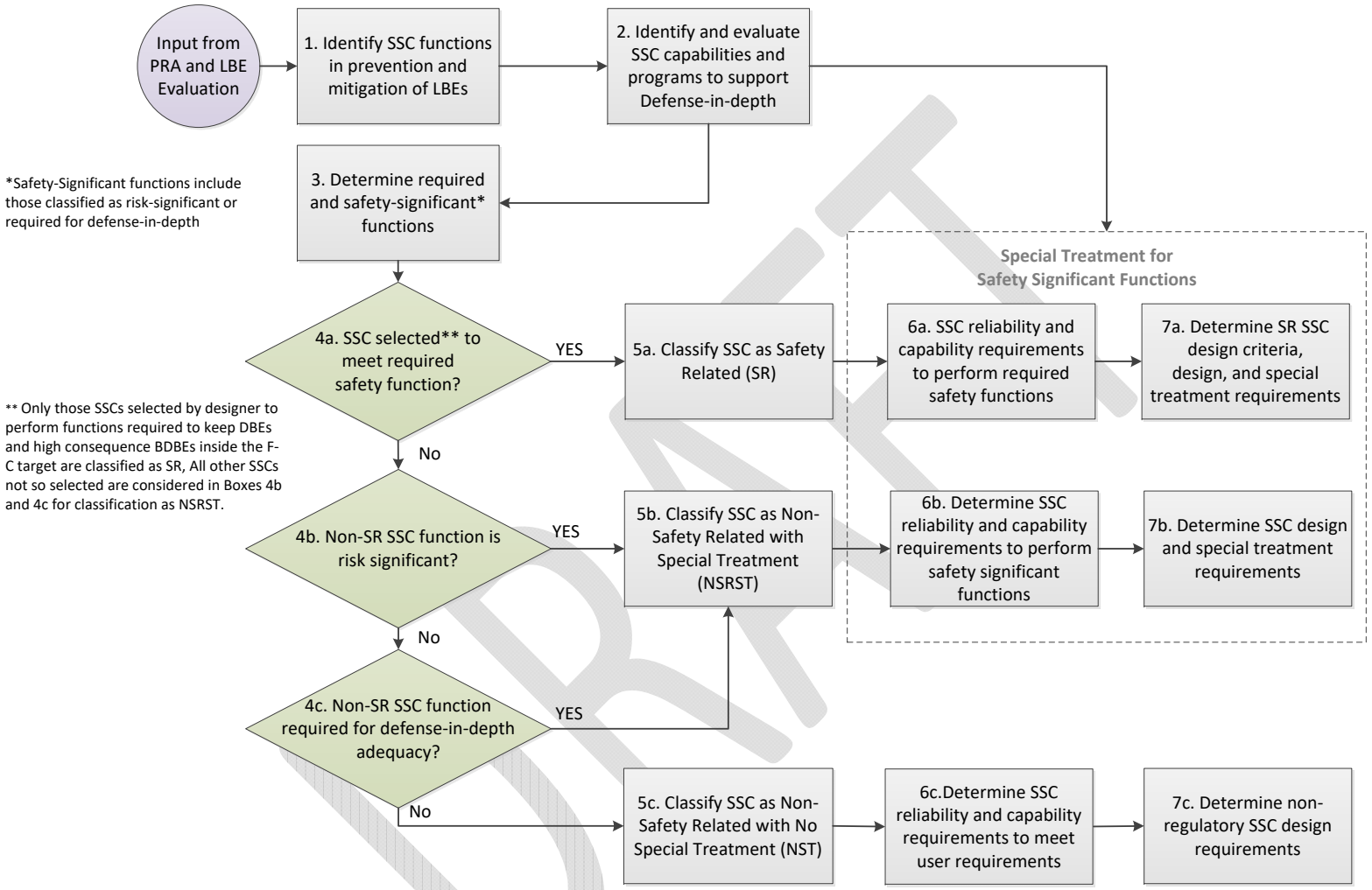

Figure 4-1. SSC Function Safety Classification Process

The SSC safety classification process is implemented in the six tasks that are described below. This process is described as an SSC function classification process rather than a SSC classification process because only those SSC functions that prevent or mitigate accidents represented in the LBEs are of concern. A given SSC may perform other functions that are not relevant to LBE prevention or mitigation or functions with a different safety classification.

Task 1: Identify SSC Functions in the Prevention and Mitigation of LBEs

The purpose of this task is to review each of the LBEs, including those in the AOO, DBE, and BDBE regions to determine the function of each SSC in the prevention and mitigation of the LBE. Each LBE is comprised of an initiating event, a sequence of conditioning events, and end state. The initiating events may be associated with an internal event such as an SSC failure or human error, an internal plant hazard such as a fire or flood, or an external event such as a seismic event or external flood.

For those internal events caused by an equipment failure, the initiating event frequency is related to the unreliability of the SSC, i.e., SSCs with higher reliability serve to prevent the initiating event. Thus, higher levels of reliability result in a lower frequency of initiating events. For SSCs that successfully mitigate the consequences of the initiating event, their capabilities and safety margins to respond to the initiating event are the focus of the safety classification process and resulting special treatment. For those SSCs that fail to respond along the LBE, their reliabilities, which serve to prevent the LBE by reducing its frequency, are the focus of the reliability requirements derived from classification and treatment process. The output of this task is the identification of the SSC prevention and mitigation functions for all the LBEs.

Task 2: Identify and evaluate SSC capabilities and programs to support defense-in-depth

The purpose of this task is to provide a feedback loop from the evaluation of defense-in-depth (DID) adequacy, which is the topic of a separate LMP white paper. This evaluation includes an examination of the plant LBEs, identification of the SSCs responsible for the prevention and mitigation of accidents, and a set of criteria to evaluate the adequacy of DID. A result of this evaluation is the identification of SSC functions, and the associated SSC reliabilities and capabilities that are deemed to be necessary for DID adequacy. Such SSCs and their associated functions are regarded as safety significant and this information is used to inform the SSC safety classification in subsequent steps.

Task 3: Determine the Required and Safety-Significant Functions

The purpose of this task is to define the safety functions that are required to meet the 10 CFR 50.34 dose requirements for all the DBEs and the high consequence BDBEs as well as other safety functions regarded as safety significant. Safety significant SSCs include those that perform risk significant functions and those that perform functions that are necessary to meet defense-in-depth criteria. The scope of the PRA includes all the plant SSCs that are responsible for preventing or mitigating the release of radioactive material. Hence the LBEs derived from the PRA include all the relevant SSC prevention and mitigation functions.

As explained previously, there are some safety functions classified as “required safety functions” that must be fulfilled to meet the F-C Target for the DBEs using realistic assumptions and dose requirements for the DBAs using conservative assumptions. In addition to these required safety functions, there are additional functions that are classified as safety significant when certain risk

significance and defense-in-depth criteria are met as explained below. In most cases, there are several combinations of SSCs that can perform these required safety functions. How individual SSC safety functions are classified relative to these function categories is resolved in Tasks 4 and 5. The concepts used to classify SSC safety functions as risk significant and safety significant are illustrated in Figure 4-2

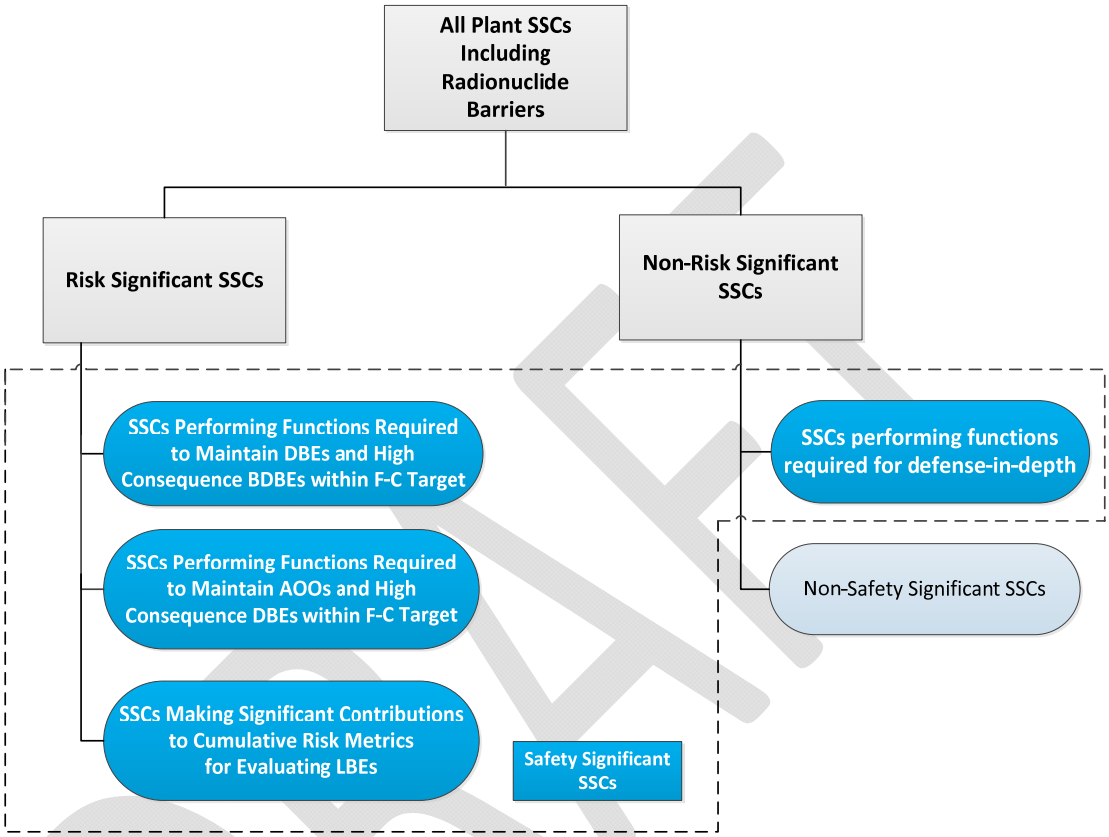

Figure 4-2. Definition of Risk Significant and Safety Significant SSCs

Tasks 4 and 5: Evaluate and Classify SSC Functions

The purpose of Tasks 4 and 5 is to classify the SSC functions modeled in the PRA into one of three safety categories: SR, NSRST, and NST.

Tasks 4A and 5A

In Task 4A, each of the DBEs and any high consequence BDBEs (i.e., those with doses above 10 CFR 50.34 limits) are examined to determine which SSCs are available to perform the required safety functions. The designer then selects one specific combination of available SSCs to perform each required safety function that covers all the DBEs and high consequence BDBEs. These specific SSCs are classified as SR in Task 5A and are the only ones credited in the Chapter 15 safety analysis of the DBAs. All the remaining SSCs are processed further in Steps 4B and 4C.

Tasks 4B and 5B

Because each SR classified SSC identified in Task 4A is necessary to keep one or more LBEs inside the F-C Target, all SR SSCs are regarded in the framework as risk significant. However,

it is also possible that some non-SR SSCs will meet the criteria for risk significance. In this task, each non-safety-related SSC is evaluated for its risk significance. A risk significant SSC function is one that is necessary to keep one or more LBEs within the F-C Target or is significant in relation to one of the LBE cumulative evaluation risk metric limits. Examples of the former category are SSCs needed to keep the consequences below the AOO limits in the F-C Target, and DBEs where the reliability of the SSCs must be controlled to prevent an increase of frequency into the AOO region with consequences greater than the F-C Target. If the SSC is classified as risk significant and is not an SR SSC, it is classified as NSRST in Task 5B. SSC functions that are neither safety-related nor risk significant are evaluated further in Task 4C.

Tasks 4C and 5C

In this task, a determination is made as to whether any of the remaining non-safety-related and non-risk significant SSC functions should be classified as requiring special treatment in order to meet criteria for defense-in-depth adequacy. Those that meet these criteria are classified as NSRST in Task 5B and those remaining as NST in Task 5C.

At the end of this task, all SSC functions reflected in the LBEs will be placed in one of the three SSC function safety classes illustrated in Figure 4-3

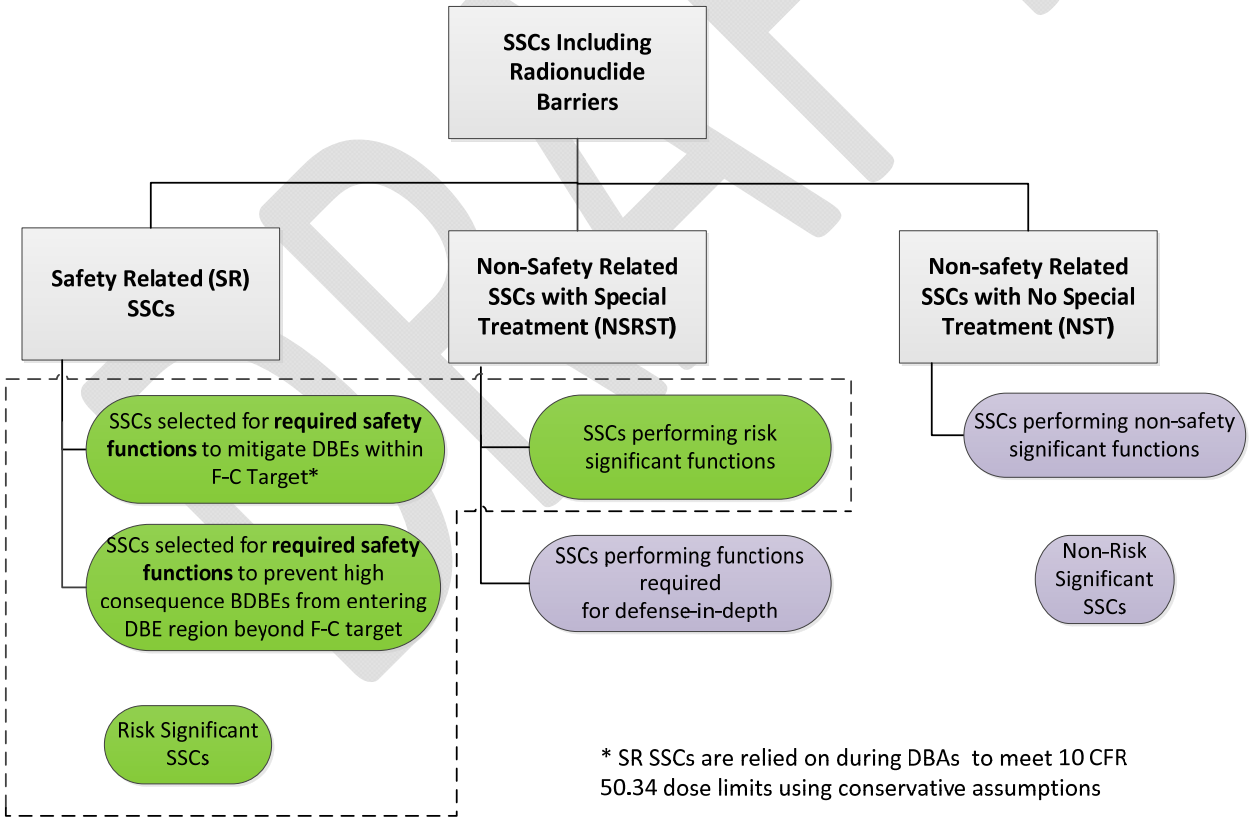

Figure 4-3. SSC Safety Categories

Note that all SSC functions classified as either SR or NSRST are regarded as "safety significant." All non-safety significant SSC functions are classified in NST.

This guidance document's approach makes use of the concept of SSC safety significance that is associated with the 10 CFR 50.69 approach and also addresses the possibility that an SSC that is not safety-related nor risk significant may be classified as safety significant based on defense-in-depth considerations. This approach to assigning risk significance uses the concept of evaluating the impact of the SSC function on the ability to meet the F-C Target, as in the previous approaches, but also includes criteria based on risk significance metrics for the cumulative risk impacts of SSC functions across all the LBEs. Hence this approach is in better alignment with the risk-informed safety classification process that is being implemented for 10 CFR 50.69.

Task 6: SSC Reliability and Capability Requirements

For each of the SSC functions that have been classified in Task 4, the purpose of this task is to define the requirements for reliabilities and capabilities for SSCs modeled in the PRA. For SSCs classified as SR or NSRST, which together represent the safety significant SSCs, these requirements are used to develop regulatory design and special treatment requirements in Task 7. For those SSCs classified as NST, the reliability and capability requirements are part of the non-regulatory owner design requirements. Examples of such requirements are discussed below and listed in Table 4-2.

For SSCs classified as SR, Functional Design Criteria (FDC) and lower level design criteria are defined to capture design-specific criteria that may supplement or may not be captured by the applicable GDC or Advanced Reactor Design Criteria. These criteria are used to frame specific design requirements as well as special treatment requirements for SR SSCs. NSRST SSCs are not directly associated with FDC but are subject to special treatment as determined by the integrated decision making process for evaluation of defense-in-depth. The FDC, design requirements, and special treatment requirements define key aspects of the descriptions of SSCs that will be included in safety analysis reports. Guidance on the development of FDC, design requirements, and special treatment requirements is found elsewhere in this guidance document.

Task 7: Determine SSC Specific Design Criteria and Special Treatment Requirements

The purpose of this task is to establish the specific design requirements for SSCs which include FDC for SR classified SSCs, regulatory design and special treatment requirements for each of the safety significant SSCs classified as SR or NSRST, and owner design requirements for NST classified SSCs. The specific SSC requirements are tied to the SSC functions reflected in the LBEs and are determined utilizing the same integrated decision making process used for evaluating the adequacy of defense-in-depth.

The term "special treatment" is used in a manner consistent with NRC regulations and Nuclear Energy Institute (NEI) guidelines in the implementation of 10 CFR 50.69. In Regulatory Guide 1.201, the following definition of special treatment is provided:

> *"…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."*

In RIEP-NEI-16, a distinction is made between special treatment as applied to safety-related SSCs and alternative special treatment afforded by 10 CFR 50.69. Alternative treatment requirements are differentiated from special treatment requirements in the use of "reasonable

confidence" versus "reasonable assurance." More details on the development of specific SSC design and performance requirements are provided in Section 3 of this guidance document.

4.2 Definition of Safety Significant and Risk-Significant SSCs

4.2.1 Safety Significant SSCs

The meaning of safety significant SSC in this framework is the same as that used in NRC regulations. The NRC glossary provides the following definition:

> *"When used to qualify an object, such as a system, structure, component, or accident sequence, this term identifies that object as having an impact on safety, whether determined through risk analysis or other means, that exceeds a predetermined significance criterion."*

4.2.2 Risk Significant SSCs

In this framework, an SSC is classified as risk significant if any of the following risk significance criteria are met for any SSC function included within the LBEs:

- A prevention or mitigation function of the SSC is necessary to meet the design objective of keeping all LBEs within the F-C Target. An LBE is considered within the F-C Target when a point defined by the upper 95th percentile uncertainty on both the LBE frequency and dose is within the F-C Target. Note that all the SR SSCs meet this criterion and hence all SR SSCs are regarded as risk significant. In addition, some non-SR SSCs perform functions that may be required to keep AOOs or high consequence DBEs within the F-C Target; these non-SR SSCs are also regarded as risk significant and classified as NSRST.
- The SSC makes a significant contribution to one of the cumulative risk metrics used for evaluating the risk significance of LBEs. A significant contribution to each cumulative risk metric limit is satisfied when total frequency of all LBEs with failure of the SSC exceeds 1% of the cumulative risk metric limit. This SSC risk significance criterion may be satisfied by an SSC whether or not it performs functions necessary to keep one or more LBEs within the F-C Target. The cumulative risk metrics and limits include:
  - The total frequency of exceeding a site boundary dose of 100 mrem shall not exceed 1/plant-year to ensure that the annual exposure limits in 10 CFR 20 are not exceeded. An SSC makes a significant contribution to this cumulative risk metric if the total frequency of exceeding a site boundary dose of 100 mrem associated with LBEs with the SSC failed is greater than 10^{-2}/plant-year.
  - The average individual risk of early fatality within 1 mile of the EAB shall not exceed 5×10^{-7}/plant-year to ensure that the NRC Safety Goal QHO for early fatality risk is met. An SSC makes a significant contribution to this cumulative metric if the individual risk of early fatalities associated with the LBEs with the SSC failed is greater than 5×10^{-9}/plant-year.
  - The average individual risk of latent cancer fatalities within 10 miles of the EAB shall not exceed 2×10^{-6}/plant-year to ensure that the NRC Safety Goal QHO for latent cancer fatality risk is met. An SSC makes a significant contribution to this cumulative risk metric if the individual risk of latent cancer fatalities associated with the LBEs with the SSC failed is greater than 2×10^{-8}/plant-year.

The cumulative risk limit criteria in this SSC classification approach are provided to address the situation where an SSC may contribute to two or more LBEs which collectively may be risk significant even though the individual LBEs may not be significant. All LBEs within the scope of the supporting PRA should be included when evaluating these cumulative risk limits. In such cases, the reliability and availability of such SSCs may need to be controlled to manage the total integrated risks over all the LBEs.

4.3 SSCs Required for Defense-in-Depth Adequacy

In this framework, an integrated decision-making process is used to evaluate the design and risk-informed decision to ensure adequacy of design and DID. Any SSCs that do not meet the risk-significance criteria will be classified as safety significant only if the integrated decision making process determines that some form of special treatment is necessary to establish the adequacy of DID. This makes sense because the DID evaluation, which will incorporate traditional engineering judgments made via an integrated decision panel, will consider additional sources of uncertainty that are not fully resolved in the PRA, including measures to enforce assumptions made in the PRA, and measures necessary to address considerations beyond the PRA. If a non-risk significant SSC is classified as safety significant, it simply means that some type of special treatment is needed to address the adequacy of DID.

As a result, the universe of safety significant SSCs in this framework includes both risk significant SSCs as well as SSCs that perform functions where some form of special treatment is determined to be needed to meet DID adequacy criteria. All safety significant SSCs are classified as SR or NSRST. All NST SSCs are not safety significant. This provides a nexus between the SSC safety classification approach and the special treatment requirements for SR and NSRST SSCs as discussed in Section 4.

4.4 Development of SSC Design and Performance Requirements

This section describes the approach for defining the design requirements for each of the three SSC safety categories: SR; NSRST; and NST. These design requirements begin with the identification of the SSC functions that are required to meet owner requirements for energy production, investment protection, worker and public safety, and licensing. SSC functions associated with the prevention and mitigation of release of radioactive material from the plant are modeled in the PRA and represented in the LBEs. The first priority in establishing the design requirements for all the SSCs associated with the prevention and mitigation of release of radioactive material is to ensure that the capability and reliability of each SSC is sufficient for all the SSC functions represented in the LBEs, including the AOOs, DBEs, BDBEs, and DBAs. A related priority is to provide reasonable confidence that the reliability and capability of the SSCs are achieved and maintained throughout the lifetime of the plant.

Those SSCs that are classified as safety-related are expected to meet applicable regulatory requirements as well as reactor-specific functional design criteria (FDC).

4.4.1 Functional Design Criteria for Safety-Related SSCs

As noted in the previous section, SSCs classified as SR perform one or more safety functions that are required to perform either of the following:

1. Mitigate DBEs within the F-C Target and DBAs within 10 CFR 50.34 dose limits
2. Prevent any high consequence BDBEs (those with doses exceeding 10 CFR 50.34 dose limits) from exceeding 1×10^{-4}/plant-year in frequency and thereby migrating into the DBE region of the F-C evaluation

These required safety functions are used within this framework to define a set of reactor-specific FDCs from which SSC regulatory design requirements may be derived. Because the FDCs are derived from a specific reactor technology and design, supported by a design specific PRA, and related to a set of design specific required safety functions, each non-LWR design would need to develop its own FDCs. A key purpose of the FDCs is to form a bridge between the safety classification of SSCs and the derivation of SSC performance and special treatment requirements.

The process for identifying the required safety functions for a given reactor starts with a review of the safety functions modeled in the PRA for the prevention and mitigation of LBEs and identifying which of those safety functions, if not fulfilled, would likely increase the consequences of any of the DBEs beyond the F-C Target. This normally involves the performance of sensitivity analyses[*] in which the performance of each safety function that mitigates the consequences of each DBE is removed and consequences re-evaluated. From the required safety functions, a top-down logical development is used to define the functional requirements that must be fulfilled for the reactor design to meet each required safety function. The FDCs may be viewed as criteria that are defined in the context of the specific reactor design features that are necessary and sufficient to meet the required safety function.

4.4.2 Regulatory Design Requirements for Safety-Related SSCs

For each of the FDCs, each designer will need to identify a set of regulatory design requirements that will be assigned to the safety-related systems assigned to perform the required safety functions.

The design requirements are performance-based and keyed to required safety functions, derived from the LBEs, and used to systematically select the safety-related SSCs.

[*] This is just one example of the use of sensitivity analyses in this framework. Sensitivity analyses are also performed in the development of the PRA and in the risk-informed and performance-based evaluation of defense-in-depth as part of the approach to addressing uncertainties in the estimation of LBE frequencies and consequences. Requirements for performing these analyses are covered in ASME/ANS-RA-S-1.4. Guidance for performing uncertainty analysis in the PRA is available in NUREG-1855. Insights from the uncertainty analysis are also an important input to the risk-informed and performance-based evaluation of defense-in-depth.

4.4.3 Evaluation of SSC Performance Against Design Requirements

Although the safety-related SSCs are derived from an evaluation of the required safety functions to mitigate the DBEs and DBAs, the safety-related and non-safety-related SSCs are evaluated against the full set of LBEs including the AOOs, and BDBEs, as well as normal plant operation, at the plant level to ensure that the F-C Target is met. This leads to design requirements for both the safety-related and non-safety-related SSCs across the full set of LBEs, including the DBAs.

4.4.4 Barrier Design Requirements

SSCs that provide functions that support the retention of radioactive material within barriers have associated regulatory design requirements that are derived from the evaluation of the LBE against the F-C Target and the FDCs. These functions include "barrier functions" in which the SSC serves as a physical or functional barrier to the transport of radionuclides and indirect functions in which performance of an SSC function serves to protect one or more other SSCs that may be classified as barriers. However, a more complete perspective on the role of barriers and the SSCs that protect each barrier needs to consider the barrier response to each of the LBEs derived from the PRA. The LBEs delineate the barrier failure modes, the challenges to barrier integrity, and the interactions between SSCs that influence the effectiveness of each barrier, and the extent of barrier independence. The evaluation of mechanistic source terms that help determine the offsite doses provides another performance metric for evaluating the effectiveness of each barrier.

When viewed across all the LBEs, each barrier plays a specific role in the retention of radionuclides; however, those roles are different in different LBEs. A full picture of the synergistic roles that each of the SSCs that comprise these barriers plays needs to consider the ways in which the SSCs mutually support the fundamental function of radionuclide retention.

It is noted that some non-LWRs employ functional barriers that are different than the physical barriers frequently employed in the past. As noted previously, in this framework, the term "barrier" is used to denote any plant feature that is responsible for either full or partial reduction of the quantity of radionuclide material that may be released during an accident. It includes features such as physical barriers or any feature that is responsible for mitigating the quantity of material, including time delays that permit radionuclide decay.

In summary, the definition of requirements for barriers cannot be fully developed simply by examining the capability of discrete physical barriers to retain radionuclides. The fact that barriers are not independent for any reactor concept precludes such a simplistic approach. A systematic development of SSC design requirements needs to consider a full spectrum of barrier challenges, barrier interactions, and barrier dependencies. A full examination of the barrier challenges, interactions and dependencies requires the performance of a technically sound PRA. Hence it is critical that the approach to formulating requirements for barriers and other SSCs be linked to a systematic identification and evaluation of LBEs supported by a PRA.

4.4.5 Special Treatment Requirements for SSCs

4.4.5.1 Purpose of Special Treatment

The purpose of special treatment is reflected in the Regulatory Guide 1.201 definition of this term:

> *"…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."*

In the context of this framework, this definition of special treatment is realized by those measures taken to provide "reasonable confidence" that SSCs will perform their functions reflected in the LBEs. The applicable functions include those that are necessary to prevent initiating events and accidents and other functions needed to mitigate the impacts of initiating events on the performance of plant safety functions. Assurance is first accomplished by achieving and monitoring the levels of reliability and availability that are assessed in the PRA and that are determined to be necessary to meet the LBE risk evaluation criteria. These measures are focused on the prevention functions of the SSCs. Assurance is further accomplished by achieving and monitoring the capabilities of the SSCs in the performance of their mitigation functions with adequate margins to address uncertainties. The relationships between SSC reliability and capability in the performance of functions that are needed to prevent and mitigate accidents are defined further in the next section.

4.4.5.2 Relationship Between SSC Capability, Reliability, Mitigation, and Prevention

The safety classification of SSCs is made in the context of how the SSCs perform specific safety functions for each LBE in which they appear. The reliability of the SSC serves to prevent the occurrence of the LBE by lowering its frequency of occurrence. If the SSC function is successful along the event sequence, the SSC helps to mitigate the consequences of the LBE.

The safety classification process and the corresponding special treatments serve to control the frequencies and consequences of the LBEs within the F-C Target and to ensure that the cumulative risk targets are not exceeded. The LBE frequencies are a function of the frequencies of initiating events from internal events, internal and external hazards, and the reliabilities and capabilities of the SSCs (including the operator) to prevent and mitigate the LBE. The SSC capabilities include the ability to prevent an initiating event from progressing to an accident, to mitigate the consequences of an accident, or both. In some cases, the initiating events are failures of SSCs themselves, in which case the reliability of the SSC in question serves to limit the initiating event frequency. In other cases, the initiating events represent challenges to the SSC in question, in which case the reliability of the SSC to perform a safety function in response to the initiating event needs to be considered. Finally, there are other cases in which the challenge to the SSC in question is defined by the combination of an initiating event and combinations of successes and failures of other SSCs in response to the initiating event. All of these cases are included in the PRA and represent the set of challenges presented to a specific SSC.

4.4.5.3 Role of SSC Safety Margins

SSC safety margins play an important role in the development of SSC design requirements for reliability and performance capability. Acceptance limits on SSC performance are set with safety margins between the level of performance that is deemed acceptable in the safety analysis and the level of performance that would lead to damage or adverse consequences for all the LBEs in which the SSC performs a prevention or mitigation function. The magnitudes of the safety margins in performance are set considering the uncertainties in performance, the nature of the associated LBEs, and criteria for adequate defense-in-depth. The ability to achieve the acceptance criteria in turn reflects the design margins that are part of the SSC capability to mitigate the challenges reflected in the LBEs.

A second example of the use of margins is in the selection of reliability performance targets. The reliability targets are set to ensure that the underlying LBE frequencies and consequences meet the LBE evaluation criteria with sufficient margins. These safety margins are also evaluated in the defense-in-depth evaluation.

A third example of safety margins is the evaluation of margins between the frequencies and consequences of the LBEs and the F-C Target and the margins between the cumulative risk metrics and the cumulative risk targets used for LBE evaluation. These risk margins are evaluated as part of the RIPB evaluation of defense-in-depth.

4.4.6 Specific Special Treatment Requirements for SR and NSRST SSCs

A summary of special treatment requirements for SSCs is provided in Table 4-1.

Table 4-1. Summary of Special Treatment Requirements for SR and NSRST SSCs

Special Treatment Category	Applicability[1] SR SSC	NSRST SSC	NST SSC	Available Guidance[4]
Requirements Associated with SSC Safety Classification				
Document basis for SSC categorization by Integrated Decision Making Panel[5]	√	√	√	Essentially the same as 10 CFR 50.69(c), Guidance in RG 1.201, NEI-00-04 for all SSCs
Document evaluation of adequacy of special treatment to support SSC categorization	√			Essentially the same as 10 CFR 50.69(d), Guidance in RG 1.201, NEI-00-04 for RISC-1 SSCs
		√		Essentially the same as 10 CFR 50.69(d), Guidance in RG 1.201, NEI-00-04 for RISC-2 SSCs
Change control process to monitor performance and manage SSC categorization changes	√	√		Essentially the same as 10 CFR 50.69(e), Guidance in RG 1.201, NEI-00-04 for RISC-1 and RISC-2 SSCs
Basic Requirements for all Safety Significant SSCs				
Reliability Assurance Program including reliability and availability targets for SSCs in performance of LBE safety functions	√	√		Essentially same as Reliability Assurance Program in SRP 17.4 for safety significant SSCs, Guidance in SRP Chapter 19.1, ASME Section XI Reliability and Integrity Management Programs
Design Requirements for SSC capability to mitigate challenges reflected in LBEs	√	√		Guidance in this guidance document, MHTGR PSID
Maintenance Program that assures targets for SSC availability and effectiveness of maintenance to meet SSC reliability targets	√	√		Essentially same as 10 CFR 50.65 Maintenance Rule; link to MR consistent with 10 CFR 50.69 for RISC-1 (SR) and RISC-2 (NSRST) SSCs
Licensee Event Reports	√	√		Essentially same as 10 CFR 50.69(f), Guidance in RG 1.201, NEI-00-04 for RISC-1 and RISC-2 SSCs
Additional Special Treatment Requirements				
Functional design criteria	√			Guidance in this guidance document, INL/EXT-14-31179
Technical Specifications	√	[2]		10 CFR 50.36, SRP, MHTGR PSID
Seismic design basis	√	[3]	[3]	Essentially the same as for existing reactors for safety-related SSCs 10 CFR 100 Appendix A
Seismic qualification testing	√			Essentially the same as for existing reactors for safety-related SSCs, 10 CFR 100 Appendix A, RG 1.100

Special Treatment Category	Applicability[1] SR SSC	NSRST SSC	NST SSC	Available Guidance[4]
Protection against design basis external events	√			Essentially the same as for existing reactors for safety-related SSCs, Guidance in 10 CFR 100 Appendix A, SRP 3
Equipment qualification testing	√			Essentially the same as for existing reactors for safety-related SSCs, 10 CFR 50.49
Materials surveillance testing	√			
Pre-service and In-service inspection via Reliability Integrity Management (RIM)	√	[2]		ASME Section XI Reliability and Integrity Management Programs. Note that the RIM program is not yet an endorsed standard, and so either an acknowledgment or refer to other available guidance (e.g., existing guidance for LWRs).
Pre-service and in-service testing	√	[2]		In–service testing needs to be integrated with Reliability Assurance Program

[1] The applicability of any category of special treatment to any SSC must be evaluated on a case-by-case basis and in the context of the SSC functions in the prevention and mitigation of applicable LBEs. This is determined via an integrated decision making process.

[2] The need for this special treatment for any NSRST is determined on a case-by-case basis and when applicable is applied to the specific functions to prevent and mitigate the applicable LBEs. This is determined via an integrated decision making process.

[3] SR classified SSCs are required to perform their safety functions following a Safe Shutdown Earthquake; NSRST SSCs are required to perform their safety functions following an Operational Basis Earthquake; NSRST and NST SSCs required to meet Seismic II/I requirements (required not to interfere with the performance of SR SSC safety functions following an Safe Shutdown Earthquake).

[4] The references in this column are mostly applicable to LWRs and hence they are offered as providing useful guidance. In this column, the term "essentially" is used to mean that non-LWR guidance under this framework will need to be developed because the referenced documents were developed specifically for LWRs in which risk insights have been "back-fit." Not all references in this column have been formally endorsed by the NRC.

[5] Integrated decision panel is discussed more fully in this guidance document on defense-in-depth and is similar to that described in NEI-00-04

The applicability of special treatment to the SSC safety categories that is identified in Table 4-1 is provided for general guidance only, and it is not prescriptive. The applicability of any special treatment to any SSC must be evaluated on a case-by-case basis and in the context of the SSC functions in the prevention and mitigation of applicable LBEs.

The purpose of any special treatment requirement is to provide adequate assurance that the SSC will perform its functions in the prevention and mitigation of LBEs. Each requirement is intended to assure that the SSC has adequate reliability and capability to perform these functions.

4.4.6.1 Reliability Assurance for SSCs

All safety significant SSCs, including those in the SR and NSRST categories, should be included in a Reliability Assurance Program (RAP) similar to that described in SRP 17.4. The reliability and availability targets established in the RAP are used to focus the selection of special treatments that are necessary and sufficient to achieve these targets and to assure they will be maintained for the life of the plant.

4.4.6.2 Capability Requirements for SSCs

All safety significant SSCs, including those in the SR and NSRST categories, should have the capability to perform the safety functions to mitigate the challenges reflected in the LBEs responsible for the safety classification. SR SSCs must be capable of mitigating the DBAs within the 10 CFR 50.34 dose limits. These SR SSCs shall include appropriate functional design criteria for such functions. Additional special treatment requirements for SR SSCs should be developed to provide assurance that the capability to perform their designated safety functions is maintained during the operating lifetime of the plant. The guiding principle is that the requirements should be performance-based and yield high confidence that the SSC functions will be performed during the identified LBEs. Specific capability requirements for other non-LWR concepts and design will necessarily be reactor technology and design specific.

Capability and reliability requirements for SR and NSRST SSCs refer back to the LBEs that challenge them so through this path some hazards, including area hazards such as pipe whip or spatial placement of a NSRST component above a SR component, may lead to specific requirements.

5.0 EVALUATION OF DEFENSE-IN-DEPTH ADEQUACY

The philosophy of defense-in-depth, 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 NRC, a formal definition that permits an objective assessment of DID adequacy has not been realized. This framework 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 assuring 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.

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

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.

5.1 Defense-in-Depth Philosophy

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

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

Figure 5-1 illustrates the concept of layers of defense embodied in this philosophy taken from NUREG/KM-0009. This framework is consistent with the "levels of defense" concept advanced by the International Atomic Energy Agency (IAEA) in Reference .

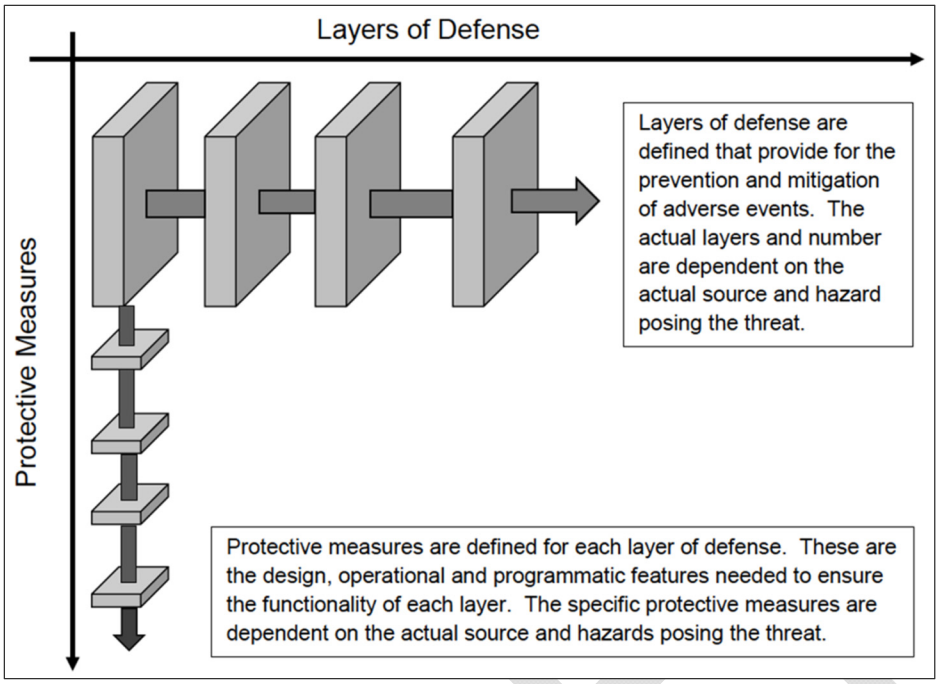

Figure 5-1. U.S. Nuclear Regulatory Commission's Defense-in-Depth Concept

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

5.2 Framework for Establishing DID Adequacy

This framework for evaluation of DID adequacy is outlined in Figure 5-2. The elements of the framework are described below.

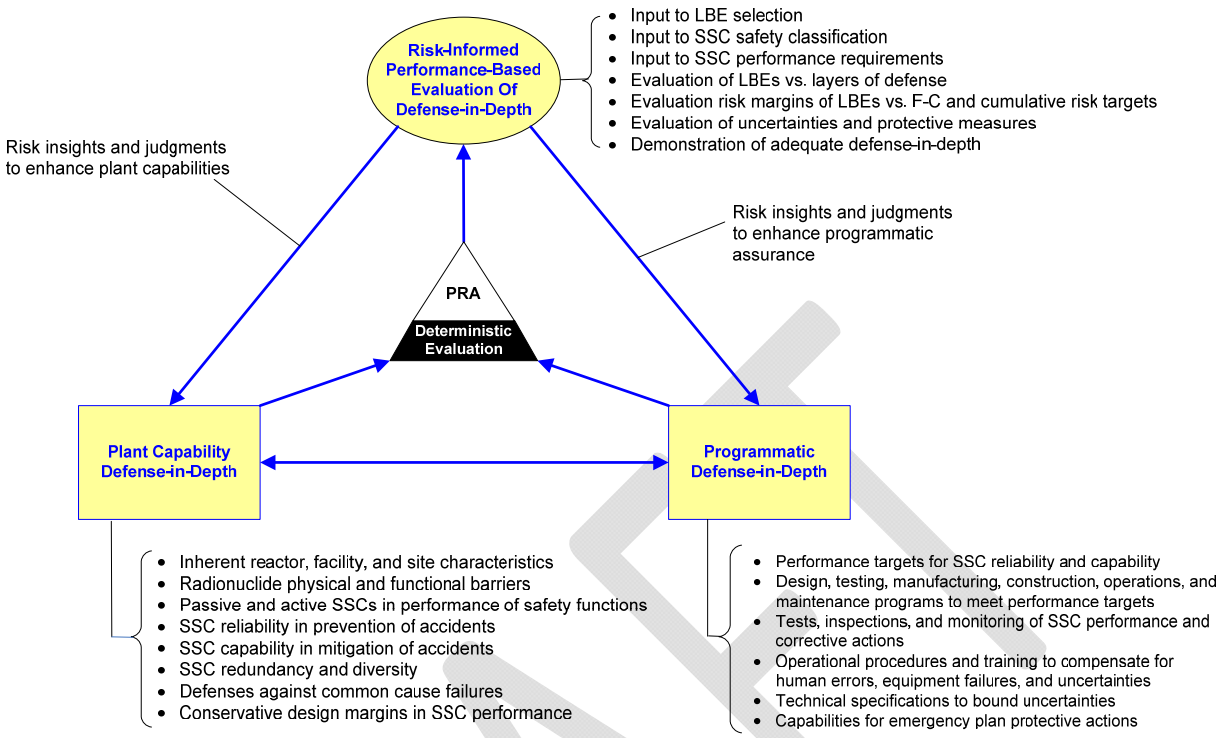

Figure 5-2. Framework for Establishing DID Adequacy

Plant Capability Defense-in-Depth

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 SSC and the use of redundancy and diversity, is important to the analysis of beyond design basis conditions that could arise. This reserve capacity to perform in severe events is consistent with the DID philosophy for conservative design capabilities that enable successful outcomes for unforeseen or unexpected events should they occur. Plant capability DID is divided into the following categories:

- Plant Functional Capability DID—This capability is introduced through systems and features designed to prevent occurrence of undesired LBE or mitigate the consequences of such events.
- Plant Physical Capability DID—This capability is introduced through SSC robustness and physical barriers to limit the consequences of a hazard.

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

Programmatic Defense-in-Depth

Programmatic DID is used to address uncertainties when evaluating plant capability DID as well as where programmatic protective strategies are defined. It is used to incorporate special treatment* during design, manufacturing, constructing, operating, maintaining, testing, and

* According to Regulatory Guide 1.201, "…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."

inspecting of the plant and the associated processes to ensure there is reasonable assurance that the predicted performance can be achieved throughout the lifetime of the plant. The use of performance-based measures, where practical, to monitor plant parameters and equipment performance that have a direct connection to risk management and equipment and human reliability are considered essential.

Risk-Informed Evaluation of Defense-in-Depth

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

This process for using the layers of defense for performing the RIPB evaluation of plant capabilities and programs, which has been adapted from the IAEA "levels of defense" approach is shown in Figure 5-3. This process is used to evaluate each LBE and to identify the DID attributes that have been incorporated into the design to prevent and mitigate accident sequences and to ensure that they reflect adequate SSC reliability and capability. Those LBEs with the highest levels of risk significance are given greater attention in the evaluation process.

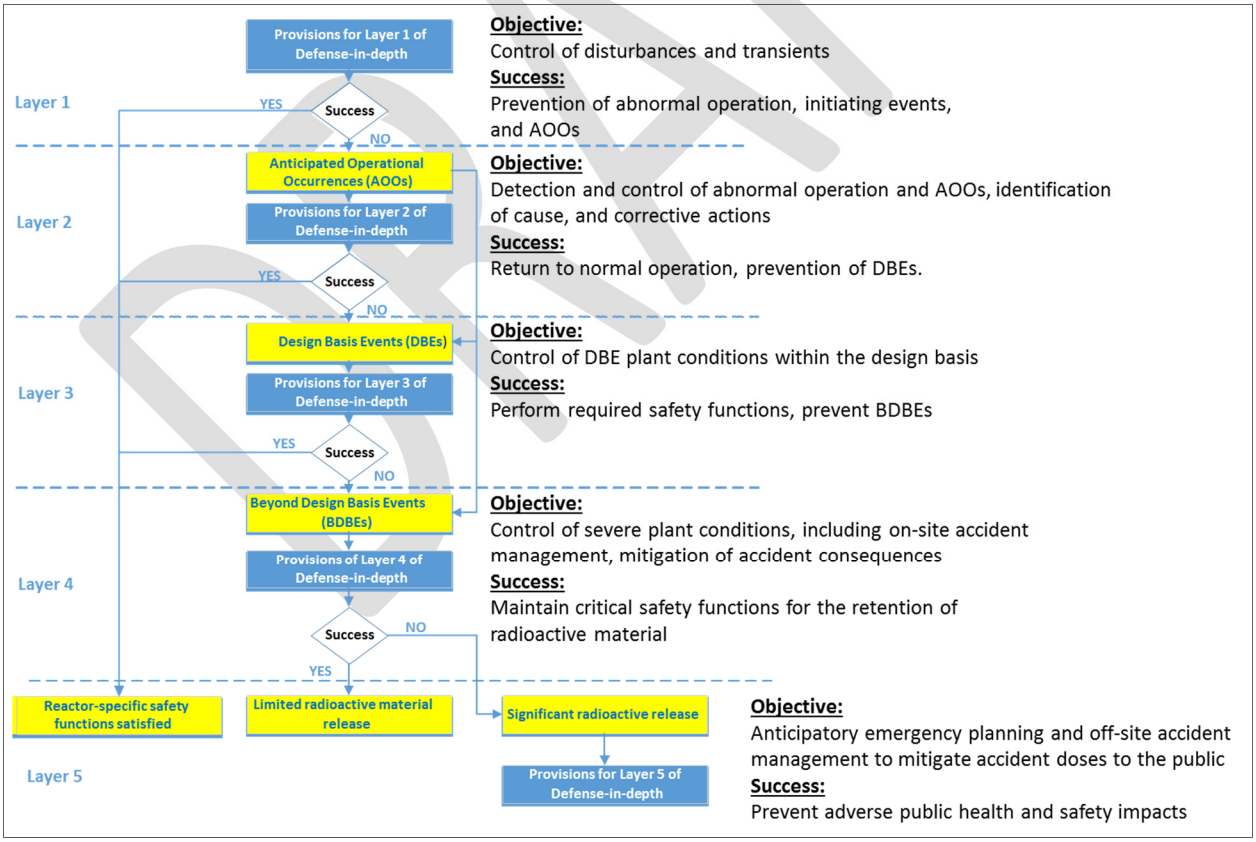

Figure 5-3. Process for Evaluating LBEs Using Layers of Defense Concept Adapted from IAEA

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 5-2. The PRA is not employed simply to calculate numerical risk metrics, but rather to develop risk insights into the design and to identify sources of uncertainty in the PRA models and supporting data that complement the deterministic elements of the framework. The DID evaluation includes the identification of compensating protective measures to address the risk significant sources of uncertainty so identified.

5.3 Integrated Framework for Incorporation and Evaluation of DID

DID is to be 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 formation of an Integrated Decision Panel (IDP) which guides the overall design effort (including development of plant capability and programmatic DID features), conducts the DID adequacy evaluation of that resulting design, and documents the DID baseline.

The incorporation of DID in each component of this framework is illustrated in Figure 5-4, and the key elements of each box in this figure are summarized below. The color coding in this figure identifies elements of the process that are probabilistic, deterministic, and risk-informed meaning having both probabilistic and deterministic aspects. It is emphasized that the implementation of the framework is not a series of discrete tasks but rather an iterative process. The sequence of boxes reflects more an information logic than a step-by-step procedure. The execution of the DID elements is accomplished in the context of an integrated decision-making process throughout the plant design and operation lifecycle.

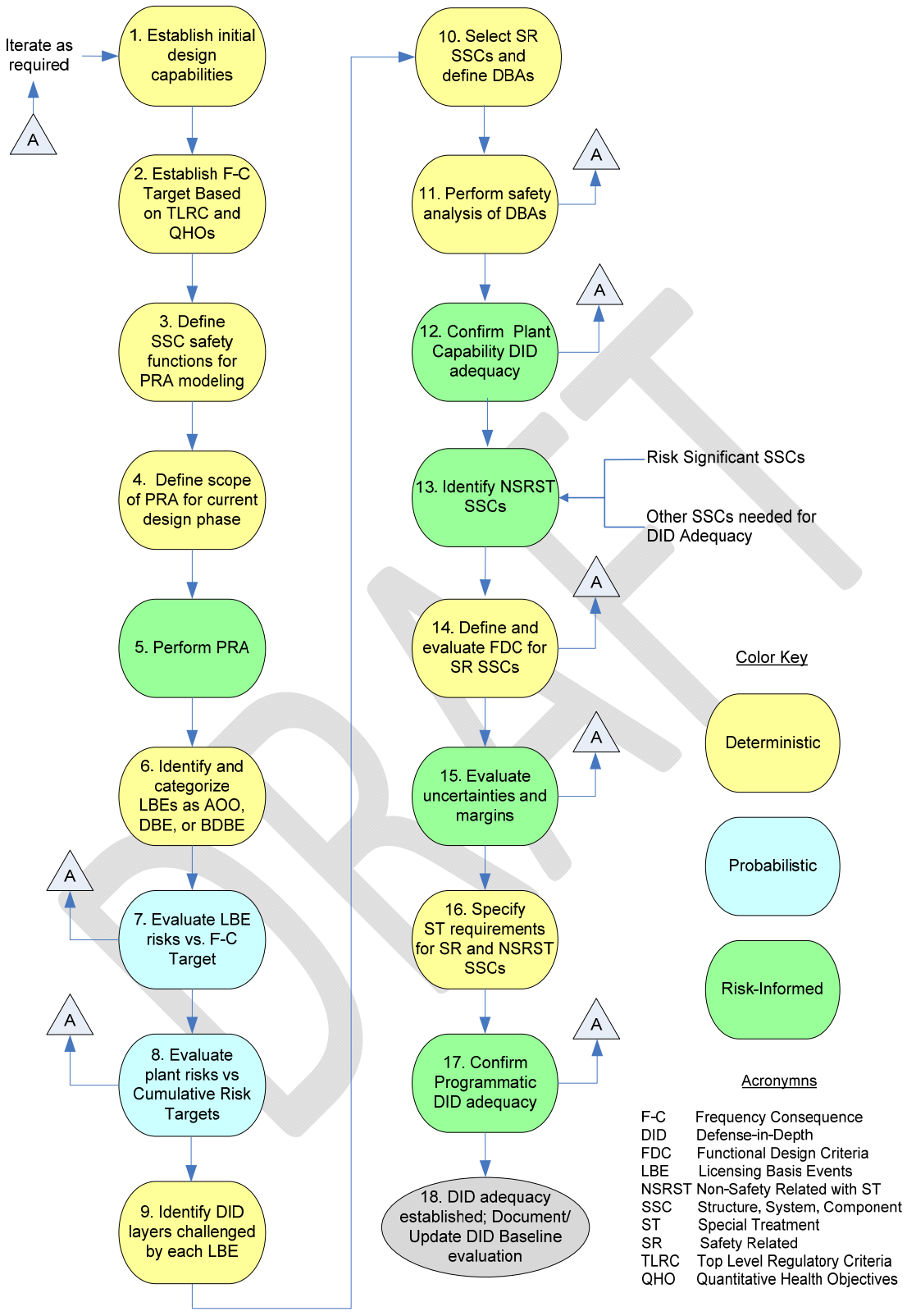

Figure 5-4. Integrated Process for Incorporation and Evaluation of Defense-in-Depth

Under this framework, an IDP will be responsible for evaluating the adequacy of DID; similar to the processes used by currently operating plants to guide risk-informed changes to the licensing basis, such as risk-informed safety classification under 10 CFR 50.69. The NEI has developed procedures and guidelines for the makeup and responsibilities of such panels. For advanced non-LWRs that are currently in various stages of design development, the IDP is comprised of a team that is responsible for implementing the integrated process steps for evaluating DID shown in Figure 5-4. This team includes those responsible for the design, operations, and maintenance program development and for performing the necessary deterministic and probabilistic evaluations identified in this figure.

Box 1. Establish Initial Design Capabilities

The process begins in Box 1 with available design information. Top level requirements are formulated with input from all stakeholders, including owner 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. Owner requirements for plant availability and reliability contribute to protecting the first layer of defense of DID in Figure 5-4 by controlling plant disturbances and preventing Initiating Events (IEs) and AOOs.

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

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

The selection of inherent reactor characteristics, primary heat transport system design parameters, and materials for SSCs dictate the safe stable operating states for the reactor.

Considerations of the need for periodic inspections and maintenance, O&M procedures, methods for starting up, shutting down, load following, and mode transitions are used to make decisions about the modes and states that need to be considered to complete the functional design and to perform the subsequent evaluations.

As part of the pre-conceptual design phase, 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 steps.

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

As noted previously, the process of establishing DID capabilities in the plant design is an iterative process. Some portions of the design advance earlier than others, normally from the nuclear island to the power conversion and site support portions. As a result, some of the activities in Figure 5-4 are updated in parallel. Thus, the IDP process recurs more often than the serial picture as more and more of the design is completed and integrated evaluations of performance and DID become more robust.

Box 2. Establish F-C Target Based on TLRC and QHOs

The F-C Target derived from TLRC is an important risk-informed element of this framework as discussed previously. The evaluation of DID adequacy in Boxes 12 and 17 of Figure 5-4 focuses on the LBEs and associated SSCs with the highest levels of risk significance.

Box 3. Define SSC Safety Functions for PRA Modeling

The plant designer defines the reactor specific safety functions as represented in Box 3. All reactors are designed to meet certain fundamental safety functions[*] such as retention of radioactive material, decay heat removal, and reactivity control. However, application of the reactor specific safety design approach leads to a set of reactor specific safety functions that achieve the fundamental safety functions. During this process, the designer confirms the allocation of these safety functions to both passive and active SSCs. In Box 3, the top-level design criteria are also confirmed for all the SSCs selected to perform the reactor specific safety functions. As Box 3 is completed the plant capabilities that support DID are largely determined.

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

Adjustments may be made to address the results of subsequent evaluations or design iterations that may expose weaknesses in design or operating assumptions, or expose margin or other uncertainties that are relevant to demonstrate adequate levels of safety and sufficient DID.

Box 4. Define Scope of PRA for Current Design Phase

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

Box 5. Perform PRA

The performance of the current phase of the PRA is covered in this box consistent with the framework described elsewhere in this guidance document. Information from the PRA is used together with deterministic inputs to establish DID adequacy as part of the risk-informed and performance-based evaluation of DID depicted in Boxes 12 and 17. The PRA is used together with traditional deterministic safety approaches to affect a risk-informed process. The PRA is not employed simply to calculate numerical risk metrics, but rather to develop risk insights into the design and to identify sources of uncertainty in the PRA models and supporting data that complement the deterministic elements of the framework. The DID evaluation includes the identification of compensating protective measures to address the risk significant sources of uncertainty so identified.

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

The process for identifying and categorizing the LBEs in terms of AOOs, DBEs, and BDBEs was discussed in detail in the LBE section above.

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

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

Box 8. Evaluate Plant Risks vs. Cumulative Risk Targets

In addition to establishing adequate margins between the risks of individual LBEs and the F-C Targets, the evaluation of the margins against the cumulative risk metrics identified previously is also necessary to establish DID adequacy

Box 9. Identify DID Layers Challenged by Each LBE

The layers of defense framework in Figure 5-3 are used in this box to evaluate each LBE with more attention paid to risk significant LBEs to identify and evaluate the DID attributes to support the capabilities in each layer and to minimize dependencies among the layers.

Box 10. Select Safety-Related SSCs and Define DBAs

The selection of SR SSCs is accomplished by examining each of the DBEs and high consequence BDBEs and performing sensitivity analyses to determine which of the safety functions modeled in these LBEs are required to perform their prevention or mitigation functions

to keep the DBEs and high consequence BDBEs inside the F-C Target. Those safety functions are classified as required safety functions. In general, there may be two or more different sets of SSCs that could provide these required safety functions. Those functions specified by the design team (represented on the IDP) select which of the available SSCs that can support the required safety functions for all the DBEs and high consequence BDBEs are designated as safety-related. DBAs are then constructed starting with each DBE and then assuming only the safety-related SSCs perform their prevention or mitigation function. DID considerations are taken into account in the selection of safety-related SSCs by selecting those that yield high confidence in performing their functions with sufficient reliability to minimize uncertainties.

Box 11. Perform Safety Analysis of DBAs

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

Box 12. Confirm Plant Capability DID Adequacy

At this step, 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 steps and guidelines for establishing the adequacy of DID. This step is supported by the results of the systematic evaluation of LBEs using the layers of defense process outlined in Figure 5-3 in Box 9. As part of the DID adequacy evaluation, each LBE is evaluated to confirm that risk targets are met without exclusive reliance on a single element of design, single program, or single DID attribute.

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

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 4. SSCs not classified as SR or NSRST are classified as NST. None of the NST SSCs are regarded as safety significant even though they may contribute to the plant capability for DID. This is true because SSCs that perform a function that prevents and/or mitigates a release of radioactive material are modeled in the PRA and are candidates for SSC classification. All of the safety significant SSCs are classified as either SR or NSRST.

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

FDC provide a bridge between the DBAs and the formulation of principle design criteria for the SR SSCs. DID attributes such as redundancy, diversity, and independence, and the use of passive and inherent means of fulfilling safety functions are used in the formulation of FDCs.

Box 15. Evaluate Uncertainties and Margins

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

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

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

Box 17. Confirm Programmatic DID Adequacy

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

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

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

The successful outcomes of Boxes 12 and 17 establish DID adequacy. This determination is made by the IDP and documented initially in a DID integrated baseline evaluation report which is subsequently revised as the iterations through the design cycles and design evaluation evolve.

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

As seen in this table, there are important DID roles in each major element of the framework.

Table 5-1. Role of Major Elements of TI-RIPB Framework in Establishing DID Adequacy

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

Evaluation of the LBEs to assure adequate functional independence of each layer of defense.

Evaluation of single features that have a high level of risk importance to assure no overdependence on that feature and appropriate special treatment to provide greater assurance of performance

Input to SSC performance requirements for reliability and capability of risk significant prevention and mitigation functions

Input to SSC performance and special treatment requirements

Integrated evaluation of the plant capability DID

Integrated evaluation of programmatic measures for DID

The IDP uses information and insights in each of these elements to support a risk-informed and performance-based evaluation of DID adequacy. As indicated in Figure 5-2, RIPB decisions that are made in this evaluation feedback any necessary changes to the DID attributes reflected in the plant capability and programmatic elements of DID.

5.5 RIPB Compensatory Action Selection and Sufficiency

Because the design, safety analyses, and PRA will be developed in phases and in an iterative fashion, the DID adequacy evaluation and baseline is updated as the design matures. The DID evaluation can be depicted as the more detailed DID framework shown in Figure 5-2 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.

5.6 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.

5.6.1 Guidelines for Plant Capability DID Adequacy

The approach to establishing plant capability DID begins in the development of the safety design approach and is accomplished in the course of the iterative process steps leading up the selection and evaluation of the licensing basis events and is also impacted by this framework to SSC safety classification. Box 7e in represents the step in the LBE evaluation where the plant capability for DID is assessed. 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 framework, a set of DID adequacy guidelines has been provided. The

guidelines can be used as a basis for initially evaluating the adequacy of plant capability DID but must be confirmed with regulators as appropriate and sufficient. These guidelines are presented in Table 5-2.

Table 5-2. Guidelines for Establishing the Adequacy of Overall Plant Capability Defense-in-Depth

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 owner 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 safety-related 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 owner requirements for plant reliability and availability and design targets for transient cycles should limit the frequency of initiating events and transients and thereby contribute to the protective strategies for this layer of DID. Quantitative and qualitative targets for these parameters are design specific.

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

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

5.6.2 DID Guidelines for Defining Safety Significant SSCs

As shown in Boxes 2 and 3 of the SSC Safety Classification process, SSCs are classified as safety significant if they perform one or more functions that are classified as risk significant, or necessary for adequacy of DID. The plant capability DID adequacy guidelines in Table 5-2 require that two or more independent plant design or operational features be provided to meet the guidelines for each LBE. Any SSCs required to meet this guideline, as determined by the IDP, would be regarded as performing a safety function necessary for adequacy of plant capability DID. Such SSCs, if classified as risk significant, would already be classified as safety significant. If one of the plant features used to meet the need for multiple DID measures in Table 5-2 involves the use of SSCs that are neither safety-related nor risk significant, the IDP would classify the SSC as safety significant and NSRST because it performs a function required for DID adequacy according to the guidelines in Table 5-2.

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 5-4 and evaluating the adequacy of DID.

5.6.3 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 design approach and ultimate finding that a plant poses no undue risk to public health and safety.

Table 5-3 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 5-3. Plant Capability Defense-In-Depth Attributes

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

5.7 Evaluation of LBEs Against Layers of Defense

A key 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. This review has the following objectives:

- 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 safety-related or non-safety-related and risk-significant 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

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

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 that need to be addressed via programmatic and plant capability DID measures have been adequately addressed.

An important consideration in the safety classification of SSCs and in the formulation of SSC performance requirements is the understanding of the roles of SSCs modeled in the PRA in the prevention and mitigation of accidents. This understanding is the basis for the formulation of the SSC capability requirements for mitigation of the challenges represented in the LBEs as well as the reliability requirements to prevent LBEs with more severe consequences. This understanding is also key to recognizing how the plant capabilities for DID achieve an appropriate balance between accident prevention and mitigation across different layers of defense, which permits an examination of the evaluation of the plant capabilities in the context of the layers of defense that were delineated in Figure 5-3.

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 5-4. This table provides an important feedback mechanism between risk-informed and performance-based evaluation of DID and plant capability DID. The event sequence framework is part of the risk-informed evaluation of DID, and the roles of SSCs in the prevention and mitigation of accidents are the result of the plant capability DID. The reliabilities and capabilities of the SSCs that prevent and mitigate events are influenced by both the plant capability and programmatic DID elements. Programmatic DID reduces the uncertainty in the reliability and capability performance of the SSCs responsible for prevention and mitigation.

Table 5-4. Event Sequence Model Framework for Evaluating Plant Capabilities for Prevention and Mitigation of LBEs

Standard Elements of Accident Sequence	Design Features Contributing to Prevention	Design Features Contributing to Mitigation
Initiating Event Occurrence	Reliability of SSCs supporting power generation reduces the IE frequencies; successful operation of the SSCs prevents the sequence.	Capabilities of normally operating systems to continue operating during disturbances to prevent initiating events serve to mitigate events and faults that may challenge these functions.

Response of Active SSCs Supporting Safety Functions: Successful and Failed SSCs	Reliability and availability of active SSCs reduce sequence frequency; successful operation of these SSCs prevents the sequence.	Capabilities of active successful SSCs including design margins reduce the impacts of the initiating events and reduce the challenges to barrier integrity.
Response of Passive Features Supporting Safety Functions: Successful and Failed SSCs	Reliability and availability of passive SSCs reduce sequence frequency; successful operation of these SSCs prevents the sequence.	Capabilities of passive successful SSCs including design margins reduce the impacts of the initiating events and reduce the challenges to barrier integrity.
Fraction of Source Term Released from Fuel	N/A	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	N/A	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	N/A	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	N/A	Inherent and passive features and capabilities of the fuel, coolant pressure boundary, and reactor building barrier including design margins conditioned on the successful response of any active or passive SSC along the sequence dictate the time available for emergency response.

The accident sequence framework for evaluating accident prevention and mitigation in Table 5-4 is used to define a simple model for estimating the risk of a release of radionuclides associated with a specific accident sequence, or LBE:

$$R_j = Q * F_{IE,j} * P_{ASSC,j} * P_{PSSC,j} * r_{fuel,j} * r_{PB,j} * r_{cont,j}$$

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.

5.7.1 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).

Margins are developed in two forms. The margins to the F-C Target are measured based on mean values of the LBE frequencies and doses. 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.

A more conservative evaluation of margins is similar to above 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.

5.7.2 Integrated Decision Panel Focus in LBE Review

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

- Is the selection of initiating events and event sequences reflected in the LBEs sufficiently complete? Are the uncertainties in the estimation of LBE frequency, plant response to events, mechanistic source terms, and dose well characterized? Are there sources of uncertainty not adequately addressed?
- Have all risk significant LBEs and SSCs been identified?
- Has the PRA evaluation provided an adequate assessment of "cliff edge effects?"
- Is the technical basis for identifying the required safety functions adequate?
- Is the selection of the SR SSCs to perform the require safety functions appropriate?
- Have protective measures to manage the risks of multi-module and multi-radiological source accidents been adequately defined?

- Have protective measures to manage the risks of all risk significant LBEs been identified, especially those with relatively high consequences?
- Have protective measures to manage the risks for all risk significant common cause initiating events such as support system faults, internal plant hazards such as fires and floods, and external hazards been identified?
- Is the risk benefit of all assigned protective measures well characterized, e.g., via sensitivity analyses?

If the evaluation identifies unacceptable answers to any of these questions, additional compensatory action would be considered, depending on the risk significance of the LBE. With reference to Figure 5-4, which identifies feedback loops in the framework at each evaluation step of the process, the compensatory action can take on different forms including changes to design and operation, refinements to the PRA, revisions to the selection of LBEs and safety classification of SSCs, as well as enhancements to the programmatic elements of DID.

5.8 Establishing the Adequacy of Programmatic DID

5.8.1 Guidelines for Programmatic DID Adequacy

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

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

Unlike the plant capabilities for DID which can be described in physical terms and are amenable to quantitative evaluation, the programmatic DID adequacy must be established using engineering judgment by determining what package of DID attributes are sufficient to meet the above objectives. These judgments are made by the IDP using the programmatic DID attributes and evaluation considerations in Table 5-5.

Table 5-5. Programmatic DID Attributes

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

The attributes of programmatic DID complement each other and provide overlapping assurance that the design plant capability is achieved in design, manufacturing, construction, and operations lifecycle phases. The evaluation focus items in Table 5-5 should be answered for each programmatic DID attribute for risk significant LBEs in order to determine that the programmatic DID provides sufficient confidence that there is reasonable assurance of adequate protection of public health and safety based on the design plant capability. The net result establishing and evaluating programmatic DID is the selection of special treatment programs for all safety significant SSCs, which include those classified as SR or NSRST.

5.8.2 Application of Programmatic DID Guidelines

In the evaluation of programmatic DID using the attributes in Table 5-5 and the questions raised in Table 5-6, the considerations discussed below will be used by the IDP.

Table 5-6. Evaluation Considerations for Evaluating Programmatic DID Attributes

Attribute	Evaluation Focus	Implementation Strategies	Evaluation Considerations
Quality / Reliability	Design Testing Manufacturing Construction O&M	Conservatism with Bias to Prevention Equipment Codes and Standards Equipment Qualification Performance Testing	1. Is there appropriate bias to prevention of AOOs progressing to postulated accidents? 2. Has appropriate conservatism been applied in bounding deterministic safety analysis of more risk significant LBEs? 3. Is there reasonable agreement between the deterministic safety analysis of DBAs and the upper bound consequences of risk-informed DBA included in the LBE set? 4. Have the most limiting design conditions for SSCs in plant safety and risk analysis been used for selection of safety–related SSC design criteria? 5. Is the reliability of functions within systems relied on for safety overly dependent on a single inherent or passive feature for risk significant LBEs? 6. Is the reliability of active functions relied upon in risk significant LBEs achieved with appropriate redundancy or diversity within a layer of defense? 7. Have the identified safety-related SSCs been properly classified for special treatment consistent with their risk significance?
Compensation for Uncertainties	Compensation for Human Errors	Operational Command and Control Practices Training and Qualification Plant Simulators Independent Oversight and Inspection Programs Reactor Oversight Program	1. Have the insights from the Human Factors Engineering program been included in the PRA appropriately? 2. Have plant system control designs minimized the reliance on human performance as part of risk-significant LBE scenarios? 3. Have plant protection functions been automated with highly reliable systems for all DBAs? 4. Are there adequate indications of plant state and transient performance for operators to effectively monitor all risk-significant LBEs? 5. Are the risk-significant LBEs all properly modeled on the plant reference simulator and adequately confirmed by deterministic safety analysis? 6. Are all LBEs for all modes and states capable of being demonstrated on the plant reference simulator for training purposes?
	Compensation for Mechanical Errors	Operational Technical Specifications Allowable Outage Times Part 21 Reporting Maintenance Rule Scope	1. Are all risk-significant LBE limiting condition for operation reflected in plant Operating Technical Specifications? 2. Are Allowable Outage Times in Technical Specifications consistent with assumed functional reliability levels for risk-significant LBEs? 3. Are all risk-significant SSCs properly included in the Maintenance Program?

Attribute	Evaluation Focus	Implementation Strategies	Evaluation Considerations
	Compensation for Unknowns (Performance Variability)	Operational Technical Specifications In-Service Monitoring Programs	1. Are the Technical Specification for risk-significant SSCs consistent with achieving the necessary safety function outcomes for the risk significant LBEs? 2. Are the in-service monitoring programs aligned with the risk-significant SSC identified through the RIPB SSC Classification process?
	Compensation for Unknowns (Knowledge Uncertainty)	Site Selection PIRT/ Technical Readiness Levels Integral Systems Tests / Separate Effects Tests	1. Have the uncertainties identified in PIRT or similar evaluation processes been satisfactorily addressed with respect to their impact on plant capability and associated safety analyses? 2. Has physical testing been done to confirm risk significant SSC performance within the assumed bounds of the risk and safety assessments? 3. Have plant siting requirements been conservatively established based on the risk from severe accidents identified in the PRA? 4. Has the PRA been peer reviewed in accordance with applicable industry standards and regulatory guidance? 5. Are hazards not included in the PRA low risk to the public based on bounding deterministic analysis?
Off-Site Response	Emergency Response Capability	Layers of Response Strategies EPZ location EP Programs Public Notification Capability	1. Are functional response features appropriately considered in the design and emergency operational response capabilities for severe events as a means of providing additional DID for undefined event conditions? 2. Is the Emergency Planning Zone (EPZ) appropriate for the full set of DBEs and BDBEs identified in the LBE selection process? 3. Is the time sufficient to execute Emergency Planning (EP) protective actions for risk significant LBEs consistent with the event timelines in the LBEs?

Quality and Reliability

The initial quality of the design is developed through the application of proven practices and application of industry codes and standards. In cases where no approved codes and standards are available, conservative adaptation of existing practices from other industries or first principles derivations of repeatable practices may be required. Conservatism should be applied in cases 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 by the IDP.

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

Margin Adequacy

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

Treatment of Uncertainty in Programmatic DID

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

Compensation for Unknowns

The layers of defense approach utilized in the DID evaluation framework includes the need to define protective measures to address unknowns. Feedback from actual operating and

maintenance experience to the PRA provides performance-based outcomes that are part of plant monitoring. Periodic PRA updates should incorporate that information into reliability (system or human) estimates to determine whether significant LBE risks have changed or new events emerged. All nuclear industry sources of information should be utilized for known, risk-significant LBEs.

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

Programmatic DID in Design

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

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

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

Examples of special treatment programs are listed in Table 5-7. The actual special treatments are established by the IDP. 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.

Table 5-7. Examples of Special Treatments Considered for Programmatic DID

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

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

5.9 Risk-Informed and Performance-Based Evaluation of DID Adequacy

5.9.1 Purpose and Scope of Integrated Decision Panel Activities

Under this framework, an IDP will be responsible for evaluating the adequacy of DID. For currently operating plants that are employing risk-informed changes to the licensing basis, such as risk-informed safety classification under 10 CFR 50.69, such panels are employed to guide the risk-informed decision-making process. The NEI has developed procedures and guidelines for the makeup and responsibilities of such panels. Specifically, NEI 00-04 Sections 9 and 11 provide valuable guidance on the composition of a panel (referred to as the Integrated Decision-Making Panel within NEI 00-04) and the associated output documentation. The decisions of the IDP should be documented and retained as a quality record; this function is critical to future decision making regarding plant changes which have the potential to affect DID.

For advanced non-LWRs that are currently in various stages of design development, the IDP is comprised of a team that is responsible for implementing the integrated process steps for evaluating DID shown in Figure 5-4. This team includes those responsible for the design, operations, and maintenance program development and for performing the necessary deterministic and probabilistic evaluations identified in this figure.

5.9.2 Risk-Informed and Performance-Based Decision Process

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

Table 5-8 provides a listing of the integrated decision-making attributes and principal evaluation focus included in the RIPB DID evaluation scope to be executed by the IDP. The RIDM process is expected to be applied at each phase of the design processes in conjunction with other integrated review processes executed during design development as described in Figure 5-4. Meeting the applicable portions of ASME/ANS PRA Standard for Advanced non-LWRs, 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 5-8. Risk-Informed and Performance-Based Decision-Making Attributes

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

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

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

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

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

5.9.3 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 5-2 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.
  - Sources of uncertainty in selection and evaluation of LBE risks are identified.
    - Completeness in selection of initiating events and event sequences is sufficient.
    - Uncertainties in the estimation of LBE frequencies are evaluated.
    - Uncertainties in the plant response to events are evaluated.
    - Uncertainties in the estimation of mechanistic source terms are evaluated.
    - Design margins in plant capabilities are adequate to address residual uncertainties.
  - Special treatment for all SR and NSRST SSCs is sufficient.

5.9.4 IDP Considerations in the Evaluation of DID Adequacy

Risk Triplet Examination

The evaluation of DID adequacy requires recurring examination of the design as it matures. Thus, there needs to a recurring consideration of the three basic questions in the risk triplet: "What can go wrong?", "How likely is it?", and "What are the consequences?" This should be done at the natural design phase review points as specific engineering information is "baselined" for the next design phase. In the reviews, hazards analysis updates, PRA updates, DBA safety analysis and plant level risk profiles (e.g. LBEs identified, changes in margins or uncertainties,

or layers of defense features, human performance assumptions, etc.) should be an explicit component of the review and decision to continue to the next engineering phase.

State of Knowledge

The level of knowledge during a design process matures from functional capabilities at plant and system levels 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 the 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 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 as a result of gaps in knowledge. DID adequacy evaluations should include both types of permanent uncertainties in reaching a final design adequacy conclusion. Attention in the evaluation of DID adequacy is paid to hazards excluded from the PRA that could either pose an on-site risk to plant or personnel performance and those that could be a risk to the public due to significant non-radiological consequences.

Magnitude of Uncertainties

DID adequacy evaluations will examine the nominal performance of the plant against various risk objectives. Evaluations will also include quantified uncertainties for PRA-derived 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 initiating events that can progressively cascade to the point of challenging public safety objectives. Initiating events that cannot cascade to a point of threating public health should be found acceptable with fewer layers of defense than events that have the potential to release large amounts of radiation.

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

5.9.5 Baseline Evaluation of Defense-in-Depth

As illustrated in Figure 5-4, there will be a number of iterations through the integrated design process to reflect different design development phases and the feedback loops indicated in Figure 5-2 where the DID evaluation leads to changes in the plant design to enhance the plant capability DID or changes to the protective measures reflected in the programmatic DID. Like many other licensing basis topics, changes in physical, functional, operational, or programmatic features require consideration of the potential for reduction of DID before proceeding. This requires that a current baseline for DID be available as a reference for change evaluation. These changes in turn require revisions to the PRA and all the subsequent steps in the integrated design process. The first complete pass through the integrated design process will require a baseline DID evaluation which completes the actions of the IDP. 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 5-9 and Table 5-10 will serve as a reminder as to the scope of the evaluation which will be documented in a controlled document.

Table 5-9. 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 5-10. Evaluation Summary – Qualitative Evaluation of Programmatic DID

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

5.9.6 Considerations in Documenting Evaluation of Plant Capability and Programmatic DID

Simplify Change Evaluation

The documentation of the DID baseline shall be derived from the design records, primarily those that verified the attributes described in previously 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 the number of layers of defense for any impacted LBEs or materially alter the effectiveness of an existing layer of defense?
- Does the change significantly increase the dependency on a single feature relied on in risk-significant LBEs?

If the answer to any of the above questions is yes, a complete evaluation of all of the DID attributes 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.

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.

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.

5.9.7 Evaluation of Changes to Defense-in-Depth

For each iteration of the design evaluation life cycle in Figure 5-4, the DID evaluation from the baseline will be re-evaluated based on a review to determine which programmatic or plant capability attributes have been affected for each layer of defense. Obviously changes that impact the definition and evaluation of LBEs, safety classification of SSCs, or risk significance of LBEs or SSCs will need to have the DID adequacy re-evaluated and the baseline updated as appropriate.

6.0 REFERENCES

Editorial placeholder; references and bibliography to be added in future draft.

7.0 GLOSSARY OF TERMS

1. Prevention
2. Mitigation
3. Prevention and mitigation balance
4. Barriers
5. Layers of defense
6. PRA technical adequacy
7. Risk significant
8. Safety significant
9. Reasonable assurance
10. Adequate protection
11. Safety design approach
12. Implementation Guidance
13. Safety Related SSC
14. Non-safety Related with Special Treatment SSC
15. Non-safety Related with No Special Treatment SSC
16. Initiating event
17. Event sequence
18. Event sequence family
19. Multi-module plant
20. Functional Design Criteria
21. Mechanistic source term (MST)
22. Safety function
23. Required safety function
24. Licensing Basis Events
25. Anticipated Operational Occurrence
26. Design Basis Event
27. Beyond Design Basis Accident
28. Design Basis Accident