WORKING DRAFT

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

Draft Report Revision N

September 28, 2018

NOTICE

Neither NEI, nor any of its employees, members, supporting organizations, contractors, or consultants make any warranty, expressed or implied, or assume any legal responsibility for the accuracy or completeness of, or assume any liability for damages resulting from any use of, any information apparatus, methods, or process disclosed in this report or that such may not infringe privately owned rights.

PROLOGUE

This guidance document represents a process for the efficient licensing of advanced non-light water reactors (non-LWRs). It is the result of a Licensing Modernization Project (LMP) led by nuclear utilities and cost-shared by the U.S. Department of Energy (DOE). The LMP prepared this document as a foundation for establishing licensing technical requirements to facilitate risk-informed and performance-based design and licensing of advanced non-LWRs. Such a process 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-LWRs. This guidance document provides one acceptable means for addressing the aforementioned topics as part of demonstrating a specific design provides reasonable assurance of adequate radiological protection.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS

ANS	American Nuclear Society
AOO*	Anticipated Operational Occurrence
ASME	American Society of Mechanical Engineers
BDBE*	Beyond Design Basis Event
CFR	Code of Federal Regulations
DBA*	Design Basis Accident
DBE*	Design Basis Event
DBEHL*	Design Basis External Hazard Level
DID*	defense-in-depth
EAB	Exclusion Area Boundary
EPA	Environmental Protection Agency
ES*	event sequence
F-C*	frequency-consequence
FDC	Functional Design Criteria
FMEA	failure modes and effects analysis
FSAR	Final Safety Analysis Report
FSF*	Fundamental Safety Function
HAZOP	hazard and operability study
IAEA	International Atomic Energy Agency
IDP	Integrated Decision-Making Panel
IE*	Initiating Event
LBE*	Licensing Basis Event
LMP	Licensing Modernization Project
LWR	light water reactor
MHTGR	a specific prismatic modular high-temperature gas-cooled reactor developed by the Department of Energy
MST*	mechanistic source term
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
PB*	performance-based
PHA	process hazard analysis
POS*	plant operating state
PRA	probabilistic risk assessment
PSF*	PRA Safety Function
QHO	Quantitative Health Objective
RAP	Reliability Assurance Program
RCPB	reactor coolant pressure boundary
RFDC*	Required Functional Design Criteria
RI*	risk-informed
RIPB	risk-informed and performance-based
RIPB-DM*	risk-informed and performance-based integrated decision-making
RSF*	Required Safety Function
SR*	Safety-Related
SRDC*	Safety-Related Design Criteria
SRP	Standard Review Plan (NUREG-0800)
SSC	structures, systems, and components
ST	Special Treatment
TI-RIPB*	technology-inclusive, risk-informed, and performance-based
TLRC	Top Level Regulatory Criteria

* These terms have special meanings defined in this document and are found in the Glossary of Terms.

1 INTRODUCTION

1.1 Purpose

This document presents a 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 (non-LWRs) 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 one 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."*

Developers of advanced non-LWRs are proposing innovative designs which promise to meet these Commission expectations. The NRC intends to achieve its mission through adherence to the principles of good regulation—independence, openness, efficiency, clarity, and reliability. The NRC staff noted in "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 nuclear regulatory infrastructure, in 1995 the Commission published "Final Policy Statement on the Use of Probabilistic Risk Assessment [PRA] 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 and 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-LWR designs. The scope of this document is focused on

establishing guidance for advanced designs so license applicants can develop inputs that can be used to demonstrate compliance with applicable regulatory requirements, including but not limited to the following:*

- 10 Code of Federal Regulations (CFR) 50.34(a) describes the content required in the Preliminary Safety Analysis Report 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.

It is noted that this TI-RIPB process does not exempt any reactor designer from existing regulations, nor does the process address all regulations applicable to nuclear power plants. Rather, the process describes an approach to inform the safety design approach which can then be applied to demonstrate compliance with the regulations applicable to a reactor design.

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

- What are the plant Initiating Events and event sequences† that are associated with the design and site?
- 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 for the protection of public health and safety?

* Note that these upper tier regulations contain requirements for reactor designers and license applicants to provide information that demonstrates compliance with other, more topic-specific regulations.

† 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 Anticipated Operational Occurrences 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 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.

- Is the philosophy of DID adequately reflected in the design and operation of the facility?

2 LICENSING BASIS DEVELOPMENT PROCESS

The overall objective of this guidance document is to describe a systematic and reproducible process for selection of LBEs, classification of SSCs, and determination of DID adequacy such that different knowledgeable parties would come to like conclusions. These outcomes are important 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 process 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 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 systematic risk assessment in combination with structured prescriptive rules to address the uncertainties which are not addressed in the risk assessment. This approach can provide reasonable assurance that adequate protection is provided for public radiological protection.

- Performance-based to evaluate effectiveness relative to realizing desired outcomes that are achieved by using quantifiable performance metrics for LBE frequencies and consequences and performance requirements for SSC capabilities to prevent and mitigate events. 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 logical, coherent, and complete bases for the development of the safety design; and, evaluation of the safety design based on the specific technology and design.

- Apply a sound PRA, including appropriate probabilistic models based on available standards, to develop and evaluate the safety design outcomes for a design.

- Answer the following broad questions:

- What are the plant Initiating Events and event sequences* 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?

In summary, the outcomes from executing the processes support developing a risk-informed and performance-based safety basis for the design and developing a safety-focused application for NRC review by systematically demonstrating 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 modeled in the PRA, hereafter referred to as PRA Safety Functions (PSFs). PSFs are defined as those functions responsible for the prevention and mitigation of an unplanned radiological release from any source within the plant.
- Collectively, the SSCs that perform the PSFs are adequately capable, reliable, diverse, and/or 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. The DID evaluation focus is to assure adequate layers of defense.
- Sufficient and integrated design decisions are made, reconciling 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 selection of LBEs.

This guidance document is organized as follows to support implementation:

- Section 3 provides a description of the LBE selection and evaluation process.

* See note regarding use of the term "accident" on Page 2.

- Section 4 provides a description of SSC classification process and derivation of performance requirements.

- Section 5 provides a description of the DID adequacy determination process.

3 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, comprising AOOs, DBEs, 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]	Anticipated event sequences expected to occur one or more times during the life of a nuclear power plant, which may include one or more reactor modules. Event sequences with mean frequencies of 1×10^{-2}/plant-year and greater are classified as AOOs. AOOs take into account the expected response of all SSCs within the plant, regardless of safety classification.
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]	Infrequent event sequences that are not expected to occur in the life of a nuclear power plant, which may include one or more reactor modules, but are less likely than AOOs. Event sequences with mean frequencies of 1×10^{-4}/plant-year to 1×10^{-2}/plant-year are classified as DBEs. DBEs take into account the expected response of all SSCs within the plant regardless of safety classification.
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]	Rare event sequences that are not expected to occur in the life of a nuclear power plant, which may include one or more reactor modules, but are less likely than a DBE. Event sequences with mean 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.
Design Basis Accidents (DBAs)	*"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 event sequences that are used to set design criteria and performance objectives for the design of Safety Related SSCs. DBAs are derived from DBEs based on the capabilities and reliabilities of Safety-Related SSCs needed to mitigate and prevent event sequences, respectively. DBAs are derived from the DBEs by prescriptively assuming that only Safety Related SSCs are available to mitigate postulated event sequence 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 has historically been expected to classify the off-normal events considered within the design basis as either AOO or DBA based on a list of historically considered events for light water reactors (LWRs) and with subjective assessment of the expected frequency of occurrence. For advanced non-LWRs, the prescriptive lists of generic LWR events are not applicable. 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 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.

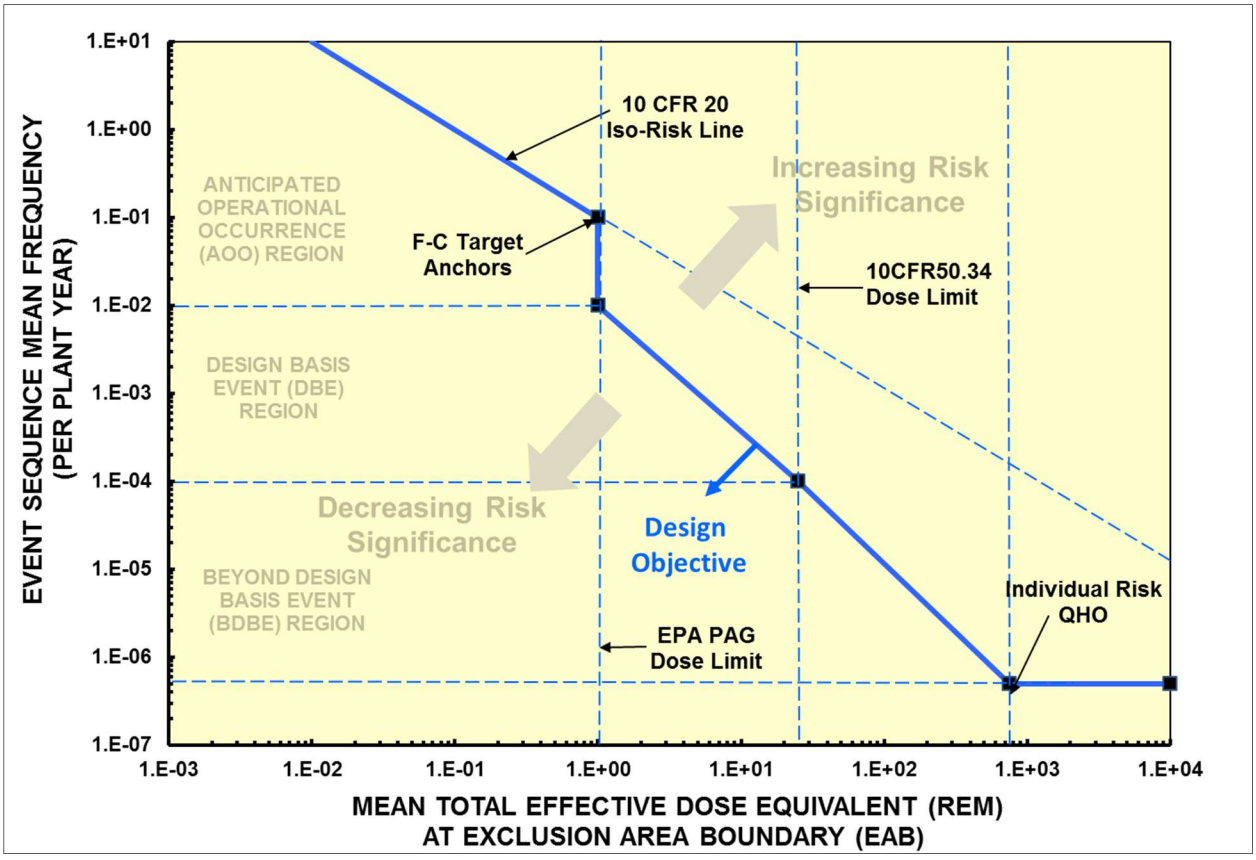

Figure 3-1. Frequency-Consequence Target

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}/plant-year, where a plant may be comprised of multiple reactor modules. DBEs are less frequent events that may be expected to occur with frequencies between 10^{-4} to 10^{-}

^{2}/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 the criteria is to evaluate the risk significance of individual AOOs, DBEs, and BDBEs, 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 Regulatory Guide 1.174 in which risk insights are used along with other factors within an integrated decision-making process.

- The F-C Target values shown in the figure should not be considered as a demarcation of acceptable and unacceptable results. The F-C Target provides a general reference to assess events, SSCs, and programmatic controls in terms of sensitivities and available margins.

- The F-C Target 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 F-C Target for lower frequency 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 the goal of avoiding the need for offsite emergency response for any AOO. It is expected that many LBEs will not result in the 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 Section 4.

- The F-C Target for DBEs range from 1 rem at 10^{-2}/plant-year to 25 rem at 10^{-4}/plant-year with the dose calculated at the Exclusion Area Boundary (EAB) for the 30-day period following the onset of the release. 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 identification of plant capabilities to prevent 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. It is expected that many LBEs will not release any radioactive material.

- 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.

- 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.

- Event sequences with 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 may also be taken into account in the RIPB evaluation of defense-in-depth.

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. The evaluation of the consequences of all LBEs are supported by mechanistic source terms.

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 AOOs, DBEs, and BDBEs does 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.

The LBEs identified in the PRA can identify important events that have the potential to release radioactivity to the public. Thus, the LBEs can inform the determination of the limiting source terms and potential releases to be considered for operational radiation protection in normal operations as well as AOOs and DBEs that can then be used to identify design-specific shielding, filtering capability of the heating, ventilation, and air conditioning system, monitoring, and other requirements for different types of non-LWRs.

3.2.2 LBE Selection Process

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

The tasks identified in Figure 3-2 do not need to be performed in any specific order and their completion is recognized to be an iterative process. In addition, the LBE selection and evaluation process may be performed using alternative tasks that provide comparable technical information as needed to identify a sufficiently complete set of design specific LBEs and to evaluate the frequencies and consequences of the LBEs against the F-C Target and cumulative risk targets. The LBE process needs to developed in a manner that facilitates the determination of risk significant LBEs and SSCs and the evaluation of

defense-in-depth adequacy. In some applications in which the DBAs and SSC safety classification steps were completed prior to the application of the LMP methodology, the evaluation of LBEs as noted in these tasks may be viewed as a means of confirming or refining prior selections in formulating the design and licensing bases.

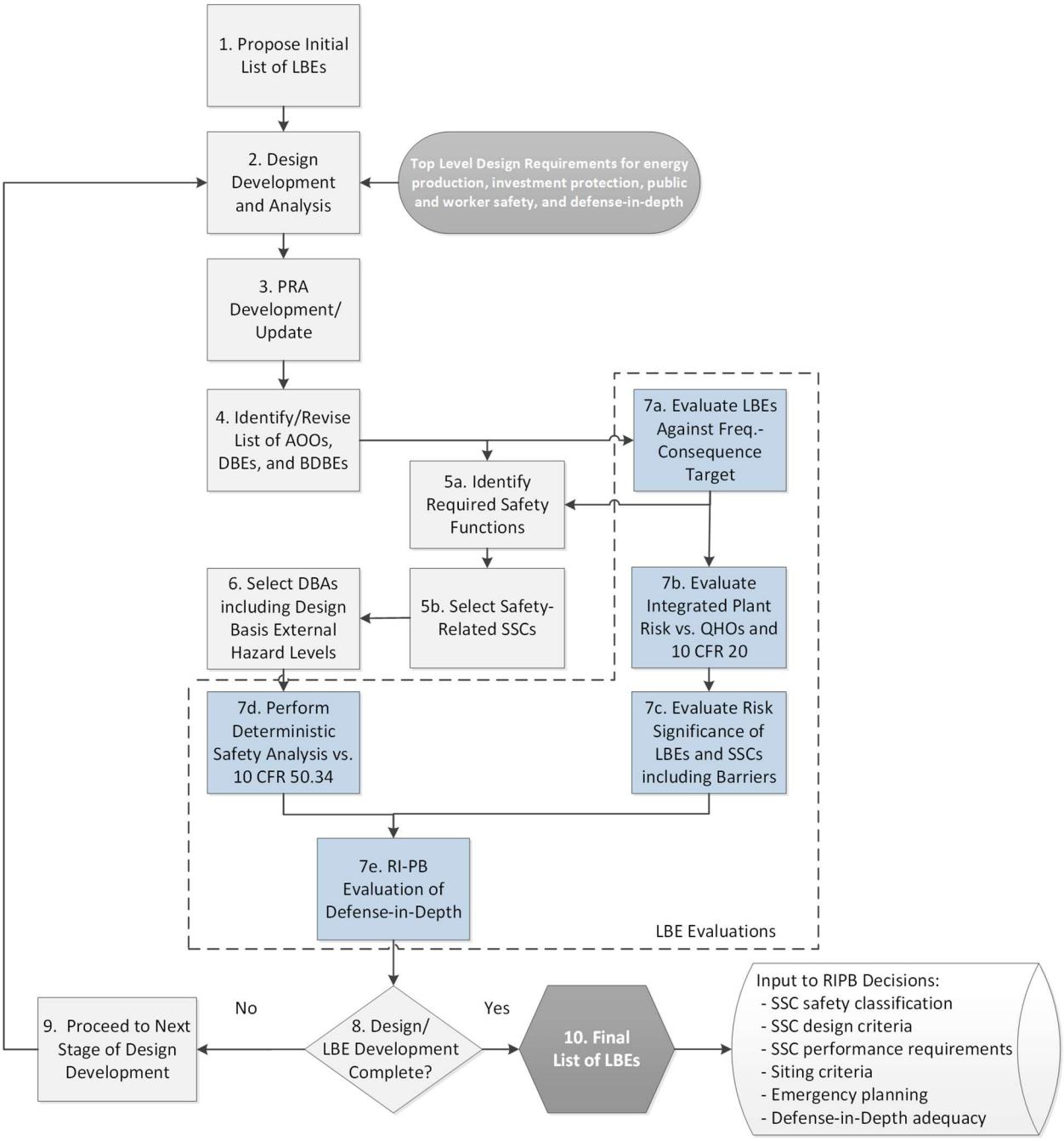

Figure 3-2. Process for Selecting and Evaluating Licensing Basis Events

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. These events are to be selected deterministically and may be supported by qualitative risk insights 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 failure modes and effects analyses (FMEAs), hazard and operability studies (HAZOPs), and Master Logic Diagrams. In many cases, the designer may also have an initial assessment regarding which SSCs may be classified as Safety-Related (SR) to meet the safety design objectives for the reactor design. This classification would also be deterministically based and may be supported by qualitative risk insights using the same information utilized for the initial selection of LBEs.

Task 2: Design Development and Analysis

Design development is performed in phases and often includes a pre-conceptual, conceptual, preliminary, and final design phase and may include iterations within phases. Design development and analysis includes definition of the elements of the safety design approach, the design features 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 SR SSCs, this process also yields the selection of SR SSCs that are needed for the deterministic safety analysis in Task 7d.

Task 3: PRA Development/Update

A PRA model is developed and then updated as appropriate for each phase of the design. Prior to the 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 plant would respond to such failure modes, and how protective strategies can be incorporated into formulating the safety design approach. The incorporation of safety analysis methods appropriate to early stages of design, such as 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 strategies or intentionally conservative analyses and related design features. If undertaken during the early design phases, the PRA is of limited scope, comprises a coarse level of detail, and makes use of engineering judgment much more than would a completed PRA that meets applicable PRA standards. The scope and level of detail of the PRA are enhanced as the design matures and siting information (or site envelope) is defined. For modular reactor designs, the event sequences modeled in the PRA should include event sequences involving single or multiple reactor modules or radionuclide sources. This approach provides useful risk insights into the design to ensure that event sequences involving multiple reactor modules are not risk-significant. The PRA process exposes sources of uncertainty encountered 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 event sequence families, each having a similar Initiating Event, challenge to the PSFs, 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 sequence families from this task 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}/plant-year, where a plant may be comprised of multiple reactor modules. DBEs are less frequent events that may occur in a plant with frequencies between 10^{-4} to 10^{-2}/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. Such insights are important inputs to the subsequent task of identifying the Required Safety Functions (RSFs). The evaluation of the consequences of LBEs is supported by mechanistic source terms.

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

Task 5a: Identify Required Safety Functions

In Task 5a, the full set of DBEs are examined to identify the PSFs 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. PSFs are those associated with the prevention or mitigation of releases from any radionuclide source within the scope of the PRA. High consequence BDBEs are those with consequences that exceed 10 CFR 50.34 dose criteria. For the DBEs these PSFs, when fulfilled, are responsible for mitigating the consequences within the F-C Target. RSFs 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 RSFs identified in Task 5a, a decision is made on which set of SSCs is selected to perform these RSFs among those found to be available on each DBE. As a result of this selection, each DBEs is protected by a set of SR SSCs to perform each RSF. Structures and physical barriers that are necessary to protect any SR SSCs in performing their RSFs in response to any design basis external event are also classified as Safety-Related. SR SSCs are also selected for any RSF associated with any high-consequence BDBEs in which the reliability of the SSC is necessary to keep the event in the BDBE frequency region. The remaining SSCs that are not classified as SR are considered in other evaluation tasks including Tasks 7b, 7c, 7d, and 7e. Performance targets and design criteria for both SR and Non-Safety-Related SSCs are developed and described more fully in Section 4.

* Designers and applicants may wish to consider "Accident Source Terms and Siting for Small Modular Reactors and Non-Light Water Reactors" (SECY-16-0012) for guidance on application of mechanistic source terms.

Task 6: Select Deterministic DBAs and Design Basis External Hazard Levels

For each DBE identified in Task 4, a deterministic DBA is defined that includes the RSF challenges represented in the DBE but assumes that the RSFs are performed exclusively by SR SSCs, and all non-safety-related SSCs that perform these same functions are assumed to be unavailable. These DBAs are then used in DBA analysis 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. The selection of conservative assumptions to be used in the DBA analysis will be informed by the quantitative uncertainty analysis of consequences that will be performed for the corresponding DBEs. In view of the fact that advanced non-LWRs will employ a diverse combination of inherent, passive, and active design features to perform the RSFs across layers of defense, and, taking into account the fact that the reactor safety design approach will be subjected to an evaluation of DID adequacy, the application of a single failure criterion is not deemed to be necessary.

A set of Design Basis External Hazard Levels (DBEHLs) will be selected to form an important part of the design and licensing basis. This will determine the design basis seismic events and other external events that the SR SSCs will be required to withstand. When supported by available methods, data, design, site information, and supporting guides and standards, these DBEHLs will be informed by a probabilistic external hazards analysis and will be included in the PRA after the design features that are incorporated to withstand these hazards are defined. Other external hazards not supported by a probabilistic hazard analysis will be covered by DBEHLs that are determined using traditional deterministic methods.

In many cases, it is expected that the initial selection of SR SSCs and selection of the DBAs will be based on a PRA that includes internal events but has not yet been expanded to address external hazards. With the understanding that SR SSCs are required to be capable of performing their RSFs in response to external events within the DBEHL, there will be no new DBAs introduced by external hazards.

Some design basis external events such as external floods or seismic events may impact multiple reactor modules concurrently; therefore, a design objective would be to prevent a substantial* release for such events.

The codes and thermal hydraulic models used within the PRA will be subject to the technical adequacy requirements in the supporting PRA standards, whereas the codes and models used in DBA analysis are expected to satisfy Regulatory Guide 1.203 requirements for evaluation models.

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 an F-C Target as shown in Figure 3-1. The figure does not define specific acceptance criteria for the analysis of LBEs but rather serves as a tool to focus the attention of the designer and those reviewing the design

* The term "substantial" is used to mean that the site boundary dose when plotted and evaluated on the F-C Target with the LBE frequency would not result in a risk-significant LBE.

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 should 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 NRC's expectations for enhanced safety. These margins also are useful in the evaluation of DID adequacy in Task 7d. The evaluations in this task are performed 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 a 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 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, and 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. These assessments apply to both the frequency and consequence estimates.

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 activity 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 compensatory measures to address those events. The evaluations in this task are based on mean frequencies and mean doses for all three LBE categories. Two exceptions to this are that BDBEs with large uncertainties in their frequencies are evaluated as DBEs when the upper 95th percentile of the frequency exceeds 10^{-4}/plant-year. 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.

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 supporting sensitivity analyses. Sources of uncertainty that are identified by the PRA and not fully resolved via quantification are addressed as part of a risk-informed evaluation of DID, as discussed in Section 5. The evaluation of the consequences of all LBEs are supported by mechanistic source terms and a quantitative uncertainty analysis.

The upper bound consequences for each DBA, defined as the 95th percentile of the uncertainty distribution, shall meet the 10 CFR 50.34 dose limit at the EAB. Sources of uncertainty in both frequencies and consequences of LBEs are identified and addressed in the LMP approach to DID.

* 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.

A function 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-reactor module or multi-source events are taken.[*]

The final element of the LBE evaluation in this task 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 process of the SSC classification task 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:

- The total frequency of exceeding a site boundary dose of 100 mrem from all LBEs should 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 mrem is selected from the annual cumulative exposure limits in 10 CFR 20.

- The average individual risk of early fatality within 1 mile of the 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 task 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 process of the SSC classification task 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

[*] 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.

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 2.5 mrem over 30 days 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 necessary to keep any LBEs inside the F-C Target, or if the total frequency of LBEs with the SSCs failed is within 1% of any of the three cumulative risk targets identified in Task 7b. This information is used to provide risk insights, to identify safety-significant SSCs, and to support the RIPB evaluation of DID 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 the DBA analysis 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 should be used to support a RIPB evaluation of DID. This task involves the identification of risk-significant sources of uncertainty in both the frequency and consequence estimates, and evaluation against DID criteria. Outcomes of this task include possible changes to the design to enhance the plant capabilities for DID, formulation of conservative assumptions for the deterministic safety analysis, and input to defining and enhancing programmatic elements of DID.

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 point for designers to assess plant features for effective satisfaction of 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 can also support related licensing matters such as defining appropriate constraints in terms of siting (i.e., 10 CFR 100, "Reactor Site Criteria"), 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-reactor module events, limit the need for restrictions on siting or emergency planning, or enhance the performance against DID criteria. The DID adequacy evaluation may result in the need for additional iterations on the adequacy of design, operational, and programmatic programs, which in turn could influence the PRA and result in a need for cycling through some or all the LBE evaluation tasks.

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 SR SSCs signifies the completion of the LBE selection process and the selection of the SR SSCs. The next task 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.

3.2.3 Evolution of LBEs Through Design and Licensing Stages

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

The early stages of design development are guided by deterministic decisions that outline the desired safety characteristics for a given design. NRC Regulatory Guide 1.232, “Developing Principal Design Criteria for Non-Light Water Reactors,” should be used as one input by designers to initially establish principal design criteria for a facility based on the specifics of its unique design.

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? Care should 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 can be defined. A review of the major systems can take place, and techniques such as a FMEA and PHAs such as 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 plant.

As the design matures, the scope and level of detail of the PRA is expanded, and it is used to help support design decisions along the way. An early simplified PRA can be very helpful in supporting design trade studies performed to better define the safety design. 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 need to be addressed. Because the design is being changed more frequently at this point and is better characterized as the design phases evolve, the PRA results and their inputs to the LBE selection process are also 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 given time, there may be systems in many design phases simultaneously. Consequently, the PRA development should be a continuum as well, maturing with the system designs. PRA updates with system development then provide a more frequent, integrated plant performance check that is otherwise missing in the conventional design process and can also provide risk insights to help the design decisions. When the design and PRA are developed in a manner that is sufficient to meet requirements reflected in applicable PRA standards and regulatory guides, the LBEs can 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 PRA results in license applications (e.g., 10 CFR 52.79). The primary motivation to utilize inputs from a PRA in the selection of LBEs is that the PRA is the only tool available that has the systematic 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 (SRP), do not refer to a systematic process for identifying design-specific events. The generic lists of events provided in the SRP as examples of transients and postulated event sequences to consider are specific to LWRs. Traditional techniques for systems analyses (i.e., FMEAs, HAZOPs, single failure analyses, etc.), which were used to define the LBEs for currently licensed reactors, 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.

Prior to the 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 plant responds to such failure modes, and how protective strategies can be incorporated into the safety design. 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 typical 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.

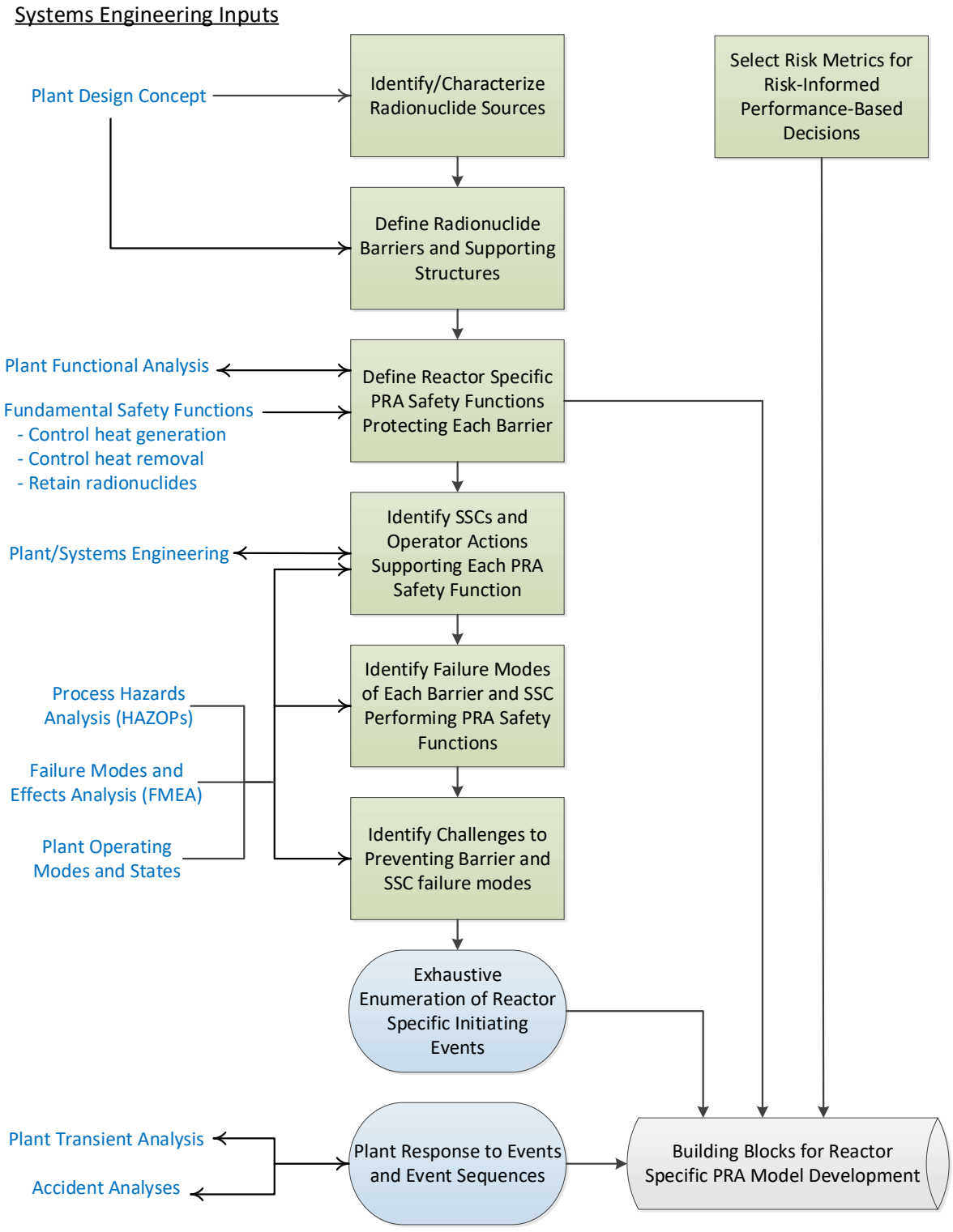

Figure 3-3. Flow Chart for Initial PRA Model Development

It should be noted that while Figure 3-3 identifies the importance of barriers due to the PRA goal of identifying event sequences that involve a release of radioactive material, the SSCs that protect these

barriers, as well as the barriers themselves, contribute to the layers of defense that are evaluated for DID adequacy in the LMP process. SSCs that perform the PRA Safety Functions that protect the barriers serve to prevent challenges to the barriers or enhance the effectiveness of barriers in preventing or limiting releases of radioactive material.

The PRA can be used to evaluate the safety characteristics of the design and to provide a structured process from which the initial set of LBEs can be risk-informed. The evaluation of the risks of the LBEs against the F-C Target helps make the LBE selection process both risk-informed and performance-based. It highlights the issues that merit the greatest attention in a safety-focused process. Subsequently, the PRA can provide important input to the formulation of performance targets for the capability and reliability of the SSCs to prevent and mitigate events 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 systematically enumerates event sequences and assesses the frequency and consequence of each event sequence. Event sequences include internal events, internal plant hazards, and external events. The modeled event sequences include the contributions from common-cause failures.

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 should 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 to feed back to the design. Selection of LBEs is facilitated by grouping many individual events into a manageable event sequence family.

The PRA's quantification of both frequencies and consequences should 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 Target. The scope of the PRA, when completed, should cover a full set of internal and external Initiating Events and provide 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 benefit from 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 and layers of defense.

If applicable, the PRA should include event sequences involving two or more reactor modules as well as two or more sources of radioactive material. This enables the identification and evaluation of risk management strategies for reactor modules and sources within the scope of a single application to ensure that sequences involving multiple reactor modules and sources are not risk-significant. The NRC staff has developed technical criteria (e.g. Quantitative Health Outcomes) for evaluating multi-reactor module risk. These technical criteria would ensure that multi-reactor module plants are designed and operated in such a way to demonstrate that the event 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-reactor 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, identified in the left side of Figure 3-3. These include FMEAs, PHAs, application of relevant experience from design and licensing of other reactors, and deterministic models of the plant response to events. 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 DID adequacy.

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 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 the DBA analysis are sufficient to meet the applicable regulatory requirements.

3.3.1 Use of PRA in LBE Selection Process

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 PSFs of the SSCs in the prevention and mitigation of events. 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—1) What can go wrong? 2) How likely is it? and 3) 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 important input in the selection of protective strategies and in the evaluation of DID 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 a risk-informed, rather than risk-based, process.

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 plant would respond to such failure modes, and how protective strategies are incorporated into formulation of the safety design approach. The incorporation of safety analysis methods appropriate to early stages of design, such as FMEA, HAZOPs, and other PHAs, 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 necessary to support this process. Reactor designs with small radionuclide inventories, few SSCs, 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 event 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 align 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 be 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 hazards expected of many non-LWR designs, especially those with low power levels, the PRA complexity necessary 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 event sequences, (regardless of reactor size or design) for which some aspects of PRA may be needed. The evaluation of the consequences of all LBEs are supported by mechanistic source terms.

3.3.4 PRA Safety Functions

A PSF, 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 RSFs 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 RSFs 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 SR SSCs to perform each RSF.

RSFs are defined starting with generic Fundamental Safety Functions (FSFs) defined by the International Atomic Energy Agency (IAEA)[*] 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

Overall Plant Risk Metrics

The PRA model can be structured differently from the model for an LWR PRA, given that plant damage states may not involve an equivalent metric to the core damage state in an LWR PRA model. Frequencies of event sequences can be individually identified and grouped into event sequence 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 and are supported by mechanistic source terms. 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 technology-inclusive 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 by considering the following approaches:

- The Initiating Events (IEs) and event sequences in the PRA delineate events involving each reactor module and radionuclide source separately as well as events involving two or more reactor modules or sources.

[*] International Atomic Energy Agency, "Proposal for a Technology-Neutral Safety Approach for New Reactor Designs," Technical Report IAEA-TECDOC-1570, 2007.

- 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 module and multi-source event sequences.

- Treatment of common-cause failures delineates those that may impact multi-reactor modules.

- The frequency basis of the event sequence quantification is events per (multi-reactor module/multi-source) plant-year.

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 5th and 95th percentiles), against the F-C Target. In this evaluation, the frequencies and consequences of individual LBEs are compared against an F-C Target derived from 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 DID adequacy. Figure 3-4 illustrates the use of the F-C Target to establish risk-significant LBEs.

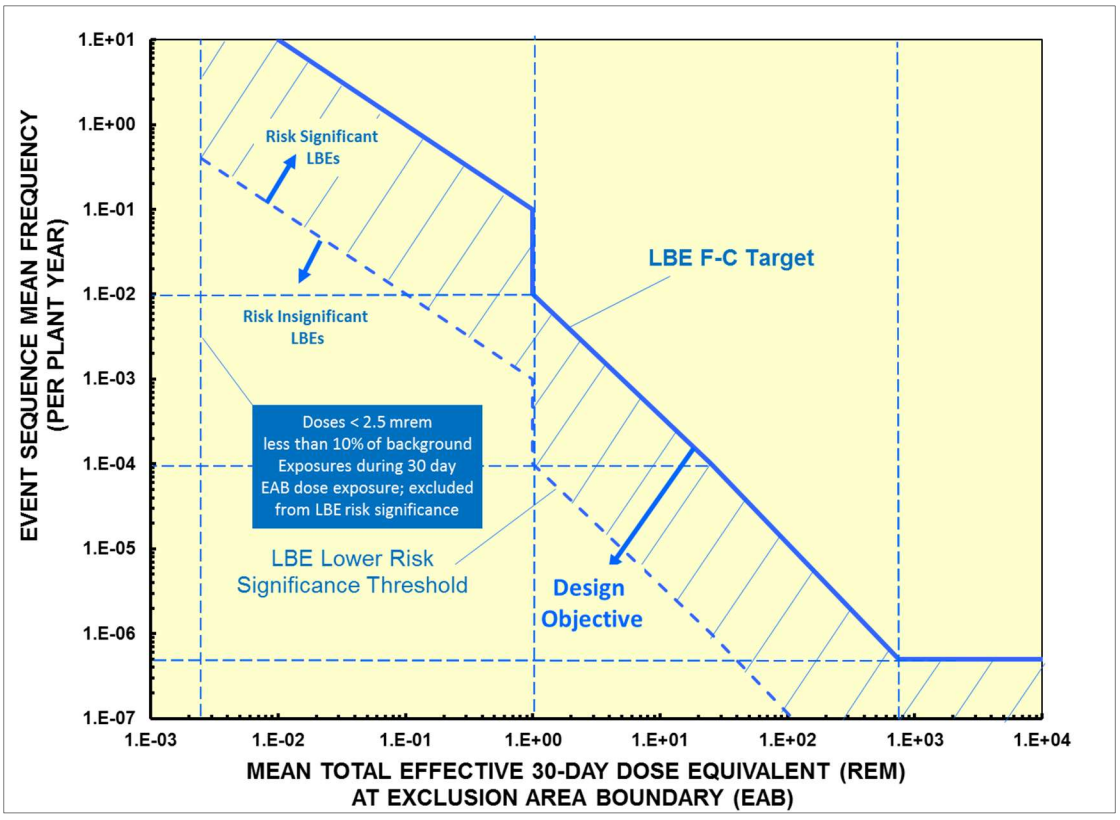

Figure 3-4. Use of the F-C Target to Define Risk-Significant LBEs

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
- 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 PSF
- 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 should 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 mrem 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 within 1% of the F-C Target with site boundary doses exceeding 2.5 mrem (see crosshatched region of Figure 3-4). 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 event 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.

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)* 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* (e.g., the event that a specific valve fails to perform its function).

Table 3-2. Risk Importance Measures

Measure	Abbreviation	Principle
Risk Reduction	RR	$R(base) - R(x_i = 0)$
Russell-Vesely	FV	$\frac{R(base) - R(x_i = 0)}{R(base)}$
Risk Reduction Worth	RRW	$\frac{R(base)}{R(x_i = 0)}$
Criticality Importance	CR	$\frac{R(x_i = 1) - R(x_i = 0)}{R(base)} \times x_i(base)$
Risk Achievement	RA	$R(x_i = 1) - R(base)$
Risk Achievement Worth	RAW	$\frac{R(x_i = 1)}{R(base)}$
Partial Derivative	PD	$\frac{R(x_i + \partial x_i) - R(x_i)}{\partial x_i}$
Birnbaum Importance	BI	$R(x_i = 1) - R(x_i = 0)$

The associated Table 3-2 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 events involving a release of radioactive material may be very small and those events with releases may involve very small source terms compared with releases from an LWR core damage event. This underlines the importance of using absolute vs. relative risk metrics to establish LBE and SSC risk significance. Hence, it is appropriate to evaluate risk significance not only on a relative basis 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-significant LBEs as illustrated in Figure 3-4. 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 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.

4 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 that are modeled in the PRA (i.e., PSFs). 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 developed for implementation of 10 CFR 50.69.

Safety classification categories are defined as follows:

- Safety-Related:
  - SSCs selected by the designer from the SSCs that are available to perform the RSFs 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 RSFs 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 there will be design requirements to protect all SR SSCs from any adverse impacts of any DBEHLs. This may lead to design requirements to prevent any adverse impacts from failure of an SSC classified as NST or NSRST that could otherwise prevent an SR SSC from performing its RSFs.

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 Task 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 PRA 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.

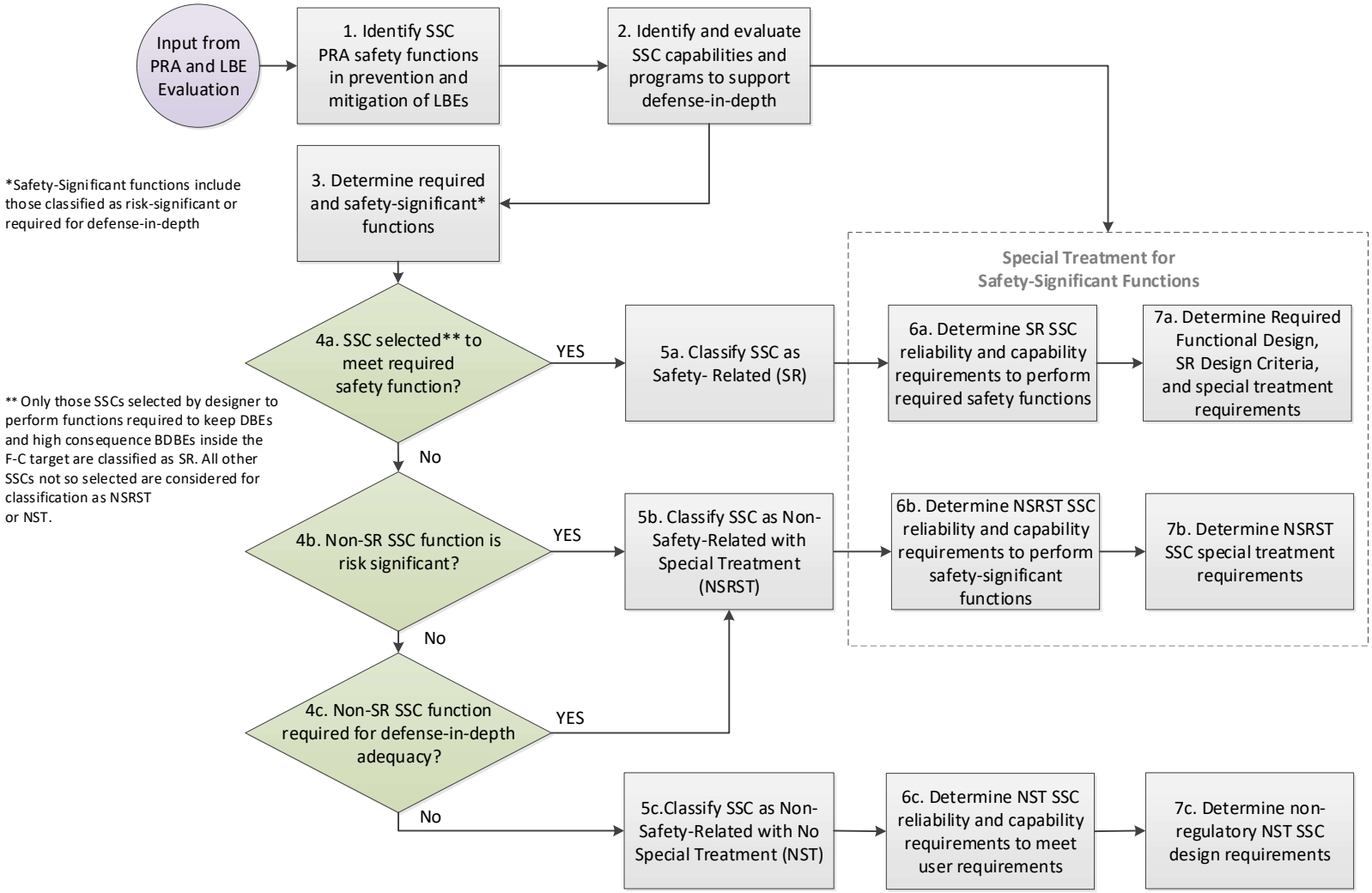

Figure 4-1. SSC Function Safety Classification Process

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 an SSC classification process because only those SSC functions that prevent or mitigate events 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 IE, a sequence of conditioning events, and an end state. The IEs 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 IE frequency is related to the unreliability of the SSC, i.e., SSCs with higher reliability serve to prevent the IE. Thus, higher levels of reliability result in a lower frequency of IEs. For SSCs that successfully mitigate the consequences of the IE, their capabilities and safety margins to respond to the IE 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 the 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 DID adequacy. This evaluation includes an examination of the plant LBEs, identification of the SSCs responsible for the prevention and mitigation of events, 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 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 tasks.

Task 3: Determine the Required and Safety-Significant Functions

The purpose of this task is to define the safety functions that are necessary to meet the F-C Target for all the DBEs and the high-consequence BDBEs, i.e., the RSFs, as well as other PSFs regarded as safety-significant. Safety-significant SSCs include those that perform risk-significant functions and those that perform functions that are necessary to meet DID 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 RSFs that must be fulfilled to meet the F-C Target for the DBEs using realistic assumptions and 10 CFR 50.34 dose requirements for the DBAs using conservative assumptions. In addition to these RSFs, there are additional functions that are classified as safety-significant when certain risk significance and DID criteria are met, as explained below. In most cases, there are several combinations of SSCs that can perform these RSFs. How individual SSC PSFs are classified relative to these function categories is resolved in Tasks 4 and 5. The concepts used to classify SSC PSFs as risk-significant and safety-significant are illustrated in Figure 4-2.

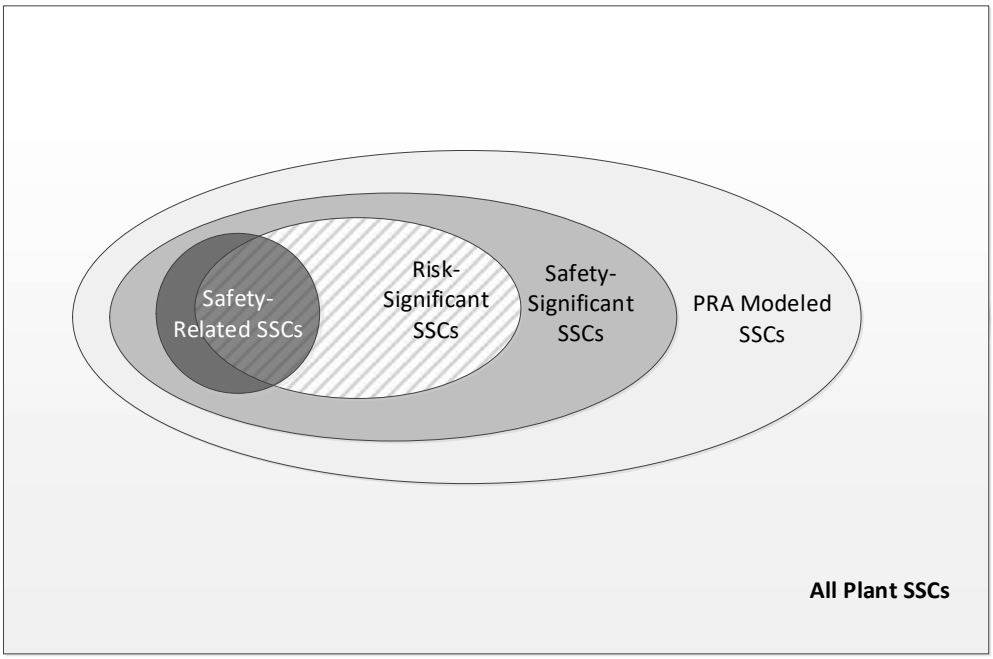

Figure 4-2. Definition of Risk-Significant and Safety-Significant SSCs

The following key points are used to define the different regions on the SSC Venn diagram:

- The PRA model does not include all the SSCs in the plant but does include any SSC that performs a prevention or mitigation function for the sources of radioactive material in the scope of the PRA.

- Safety-significant SSCs are within the scope of the PRA-modeled SSCs and include SSCs that perform a risk-significant function and those that are needed to meet DID criteria.

- Safety-Related SSCs may or may not be risk-significant depending on whether they meet the SSC risk significance criteria. While SR SSCs perform RSFs that are needed to keep one or more DBEs or high-consequence BDBEs within the F-C Target, if there is sufficient redundancy or diversity provided by other SSCs that perform these RSFs, a given SR SSC is not necessarily risk-significant. However, all SR SSCs contribute to the layers of defense in meeting the DID adequacy criteria, and all SR SSCs are classified as safety-significant.

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 RSFs. The designer then selects one specific combination of available SSCs to perform each RSF that covers all the

DBEs and high-consequence BDBEs. These specific SSCs are classified as SR in Task 5A and are the only ones included in the DBA analysis of the DBAs. All remaining SSCs are processed further in Tasks 4B and 4C.

Tasks 4B and 5B

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 should 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 SR 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 DID 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 can be placed in one of the three SSC function safety classes illustrated in Figure 4-3.

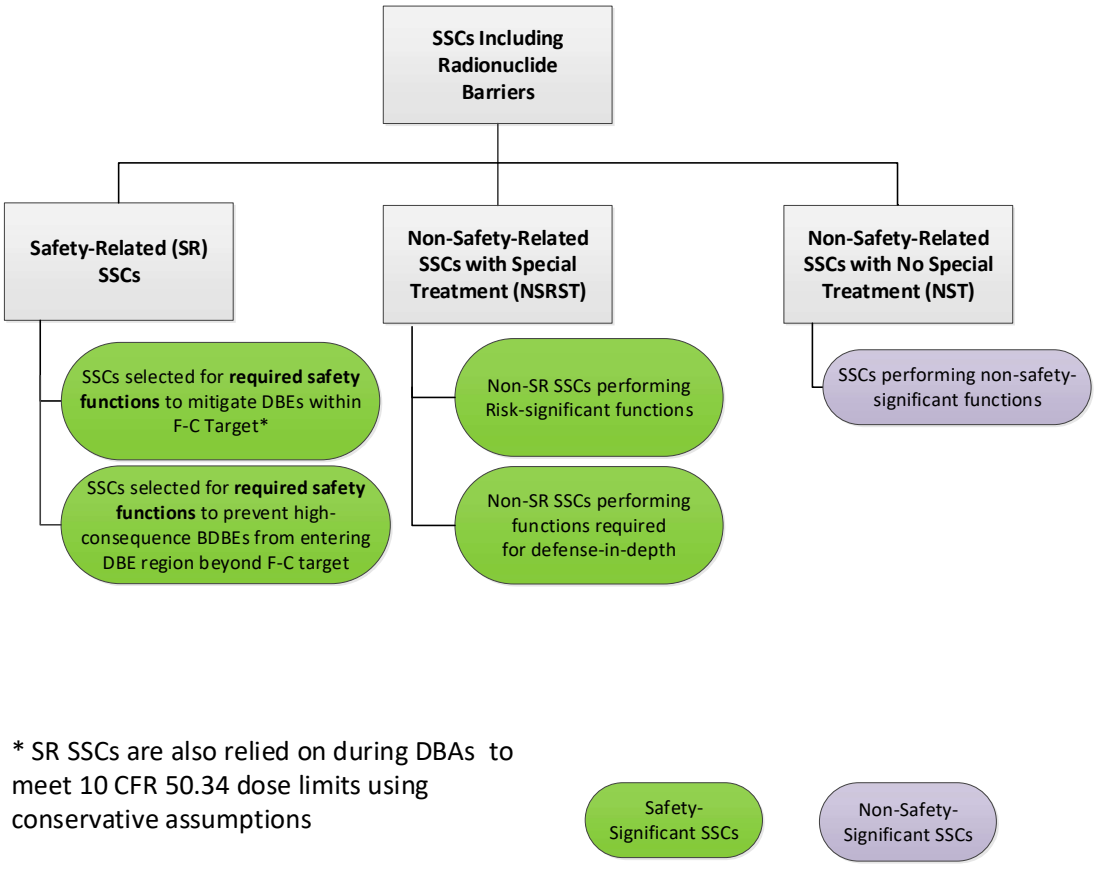

Figure 4-3. SSC Safety Categories

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

This guidance document makes use of the concept of SSC safety significance that is associated with 10 CFR 50.69 and also addresses the possibility that an SSC that is not SR nor risk-significant may be classified as safety-significant based on DID 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, and also includes criteria based on risk significance metrics for the cumulative risk impacts of SSC functions across all the LBEs.

Task 6: SSC Reliability and Capability Requirements

For each of the SSC functions 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 specific 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.

In order to meet the risk targets (F-C Target and cumulative risk targets), SSCs that are relied upon will need to meet strict reliability performance targets and will need to demonstrate DID adequacy. Strategies to achieve design reliability targets include use of passive and inherent design features, redundancy, diversity, and defenses against common-cause failures. Programmatic actions would be used to maintain performance within the design reliability targets.

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 design criteria 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 DID adequacy.

For SSCs classified as SR, the design criteria are referred to as Safety-Related Design Criteria (SRDC). These are derived from the Required Functional Design Criteria (RFDC) that are in turn developed from the RSFs determined in the LBE selection process as discussed in Section 3 of this guidance. RSFs are those safety functions that must be fulfilled to keep the DBEs within the F-C Target. RFDCs are taken down to a lower level and form a transition to SSC-level criteria. RFDCs are defined to capture design-specific criteria that may be used to supplement or modify the applicable General Design Criteria or Advanced Reactor Design Criteria in the formulation of Principal Design Criteria. RSFs and RFDCs are technology- and design-specific and are framed at the function level. After SR SSCs have been selected to perform the RSFs, the SRDCs are defined at the SSC level in a manner that assures meeting the RFDCs and the RSFs for the specific SSC selected to perform the RSFs.

NSRST SSCs are not directly associated with RFDC but are subject to special treatment as determined by the integrated decision-making process for evaluation of DID and for meeting the reliability and capability requirements set in Task 6. The RFDC, SRDC, the reliability and capability requirements for SR and NSRST SSCs, and special treatment requirements for SR and NSRST SSCs define safety-significant aspects of the descriptions of SSCs that should be included in safety analysis reports.

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 SR 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," which is a general conclusion in initial plant licensing. More details on the development of specific SSC design and performance requirements are provided in Section 4.4 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 process 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

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. In addition, some non-SR SSCs perform functions that may be necessary to keep AOOs or high-consequence DBEs within the F-C Target; these non-SR SSCs are also regarded as risk-significant and are 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 should 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 process are provided to address the situation in which an SSC may contribute to two or more LBEs that 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 process, 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 should 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 incorporates traditional engineering judgments made via an integrated decision-making panel, will consider additional sources of uncertainty that are not fully resolved in the PRA, including measures to enforce assumptions made in the PRA, that may impact both frequencies and consequences and measures necessary to address considerations beyond the PRA. If a non-risk-significant SSC is classified as safety-significant, it means that some type of special treatment should be applied to support the adequacy of DID.

As a result, the universe of safety-significant SSCs 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.

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 necessary 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 are 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 are 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 SR are expected to meet applicable regulatory requirements as well as reactor-specific and design-specific SRDC derived from the RFDC.

4.4.1 Required Functional Design Criteria for Safety-Related SSCs

As noted previously, 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 RSFs are used within this process to define a set of reactor-specific RFDCs from which SRDCs may be derived. Because the RFDCs are derived from a specific reactor technology and design, supported by a design-specific PRA, and related to a set of design specific RSFs, each non-LWR design would require the development of a unique set of RFDCs. One purpose of the RFDCs is to form a bridge between the safety classification of SSCs and the derivation of SSC performance, special treatment requirements, and SRDCs.

The process for identifying the RSFs 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 PSFs, if not fulfilled, would likely increase the consequences of any of the DBEs beyond the F-C Target. This normally involves implementation of sensitivity analyses[*] in which the performance of each PSF that mitigates the consequences of each DBE is removed and consequences re-evaluated. From the RSFs, a top-down logical development is used to define the functional requirements that must be fulfilled for the reactor design to meet each RSF. The RFDCs may be viewed as functional criteria that are defined in the context of the specific reactor design features that are necessary and sufficient to meet the RSF. The corresponding SRDCs are then developed from the RFDCs.

4.4.2 Regulatory Design Requirements for Safety-Related SSCs

For each of the RFDCs, each designer should identify a set of SRDCs appropriate to the SR SSCs assigned to perform the RSFs.

The design requirements are performance-based and tied to RSFs, derived from the LBEs, and used to systematically select the SR SSCs.

[*] This is just one example of the use of sensitivity analyses in this process. Sensitivity analyses are also performed in the development of the PRA and in the RIBP evaluation of DID as part of the approach to addressing uncertainties in the estimation of LBE frequencies and consequences, including uncertainties in the mechanistic source terms. 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 RIPB evaluation of DID.

4.4.3 Evaluation of SSC Performance Against Design Requirements

Although the SR SSCs are derived from an evaluation of the RSFs to mitigate the DBEs and DBAs, the SR 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 SR 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 RFDCs. 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 within a given layer of defense and the extent of independence among layers of defense. The evaluation of mechanistic source terms that help determine the offsite doses provides another performance metric for evaluating the effectiveness of each barrier within a given layer of defense.

When viewed across all the LBEs, each barrier plays a specific role within a given layer of defense 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 layers of defense plays must consider the ways in which the SSCs mutually support the FSF of radionuclide retention.

It is noted that some non-LWRs employ functional barriers that are different from the physical barriers frequently employed in the past. As noted previously, in this process, the term “barrier” is used to denote any plant feature within a given layer of defense that is responsible for either prevention of radionuclide release or reduction in the quantity of radionuclide release during an event. It comprises physical barriers and any other features that are responsible for mitigating the quantity of material released, 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. It is important to assure that barriers and other contributions to layers of defense are functionally independent. A systematic development of SSC design requirements must consider a full spectrum of barrier challenges, barrier interactions, and barrier dependencies within layers of defense. A full examination of the barrier challenges, interactions and dependencies requires the performance of a technically sound PRA. Hence, it is logical 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

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 process, 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 IEs and event sequences and other functions needed to mitigate the impacts of IEs on the performance of PSFs. 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 event sequences are defined further in the next section.

The activities above are a subpart of the overall set of programmatic activities included design, manufacturing, construction, and operations of the plant that provide greater assurance that the plant capabilities and performance outcomes remain within the design basis. The broader list of possible programmatic actions shown in Table 4-1 are evaluated as part of the DID adequacy evaluation described in Section 5. The actual set of special treatments applied to a given SSC are influenced by RIPB considerations as described in the following discussion.

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

Special Treatment Category	Applicability[1]			Available Guidance[4]
	SR SSC	NSRST SSC	NST SSC	
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 Regulatory Guide 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 Regulatory Guide 1.201, NEI-00-04 for RISC-1 SSCs
		√		Essentially the same as 10 CFR 50.69(d), Guidance in Regulatory Guide 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 Regulatory Guide 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 PRA 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 Preliminary Safety Information Document
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 Regulatory Guide 1.201, NEI-00-04 for RISC-1 and RISC-2 SSCs
Additional Special Treatment Requirements				
Required Functional Design Criteria	√			Guidance in this guidance document, INL/EXT-14-31179
Technical Specifications	√	[2]		10 CFR 50.36, SRP, MHTGR Preliminary Safety Information Document
Seismic design basis	√	[3]	[3]	Essentially the same as for existing reactors for SR SSCs 10 CFR 100 Appendix A

Special Treatment Category	Applicability[1]			Available Guidance[4]
	SR SSC	NSRST SSC	NST SSC	
Seismic qualification testing	√			Essentially the same as for existing reactors for SR SSCs, 10 CFR 100 Appendix A, Regulatory Guide 1.100
Protection against design basis external events	√			Essentially the same as for existing reactors for SR SSCs, Guidance in 10 CFR 100 Appendix A, SRP 3
Equipment qualification testing	√			Essentially the same as for existing reactors for SR SSCs, 10 CFR 50.49
Materials surveillance testing	√			
Pre-service and risk-informed in-service inspections	√	[2]		See Regulatory Guide 1.178.
Pre-service and in-service testing	√	[2]		In–service testing needs to be integrated with Reliability Assurance Program.

[1] The applicability of each category of special treatment to any SSC is indicated by the check marks in this table. The specific requirements for each applicable category should 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 in the design and confirmed 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 RSFs following a Safe Shutdown Earthquake; NSRST and NST SSCs required to meet Seismic II/I requirements (required not to interfere with the performance of SR SSC RSFs following a 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 process may 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-Making Panels are discussed more fully in this guidance document and are similar to those described in NEI-00-04.

Relationship Between SSC Capability, Reliability, Mitigation, and Prevention

The safety classification of SSCs is made in the context of how the SSCs perform specific PSFs 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 resulting from internal events, internal hazards, and external hazards, as well as 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 event sequence, to mitigate the consequences of an event sequence, 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 PSF in response to the Initiating Event must 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.

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 DID. 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 assessed in the DID 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 assessed as part of the RIPB evaluation of DID.

Specific Special Treatment Requirements for SR and NSRST SSCs

The applicability of special treatment to the SSC safety categories 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 should 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.

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 are maintained for the life of the plant.

Capability Requirements for SSCs

All safety-significant SSCs, including those in the SR and NSRST categories, should have the capability to perform the PSFs 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 RFDC for such functions. Additional special treatment requirements for SR SSCs should be developed to provide assurance that the capability to perform their RSFs is maintained during the operating lifetime of the plant. The guiding principle is that the requirements should be performance-based and should yield high confidence that the SSC functions are performed during the identified LBEs.

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 an SR component, may lead to specific requirements.

5 EVALUATION OF DEFENSE-IN-DEPTH ADEQUACY

The philosophy of defense-in-depth, multiple independent but complimentary means 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 process provides an approach that permits the establishment of DID in design, construction, maintenance, and operation of nuclear facilities. This is accomplished by the reactor designer and operator with the objective of 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 LBEs, 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.

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 process is consistent with the "levels of defense" concept advanced by the 2005 IAEA Safety Report Series No. 46, "Assessment of Defense in Depth for Nuclear Power Plants."

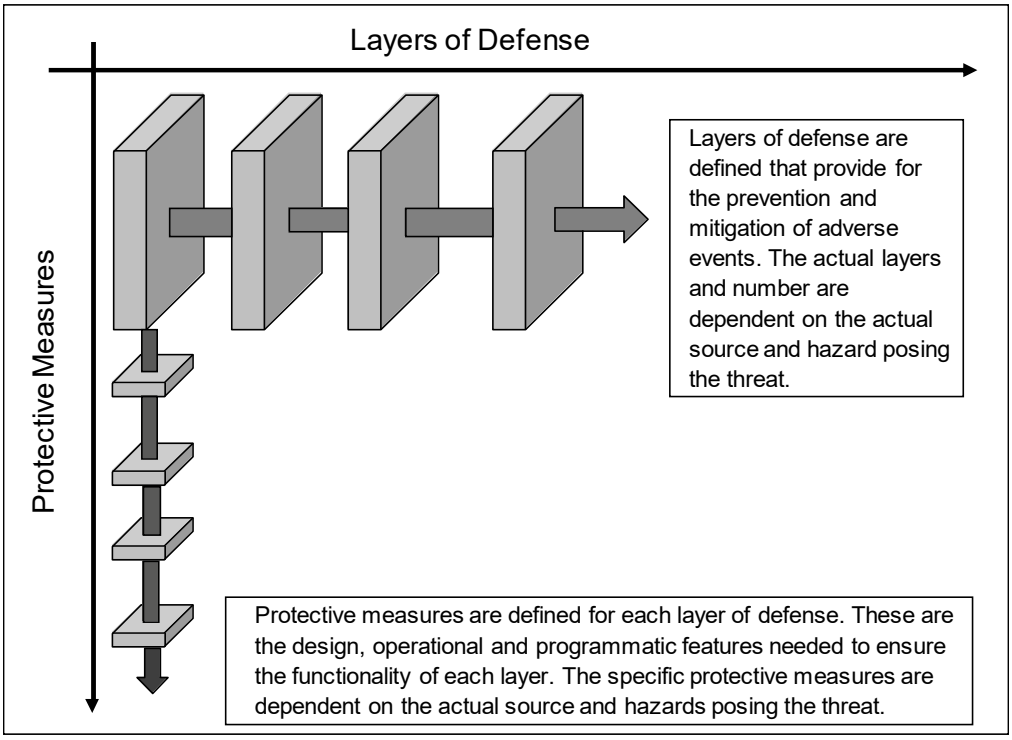

Figure 5-1. U.S. Nuclear Regulatory Commission's Defense-in-Depth Concept

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

5.2 Framework for Establishing DID Adequacy

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

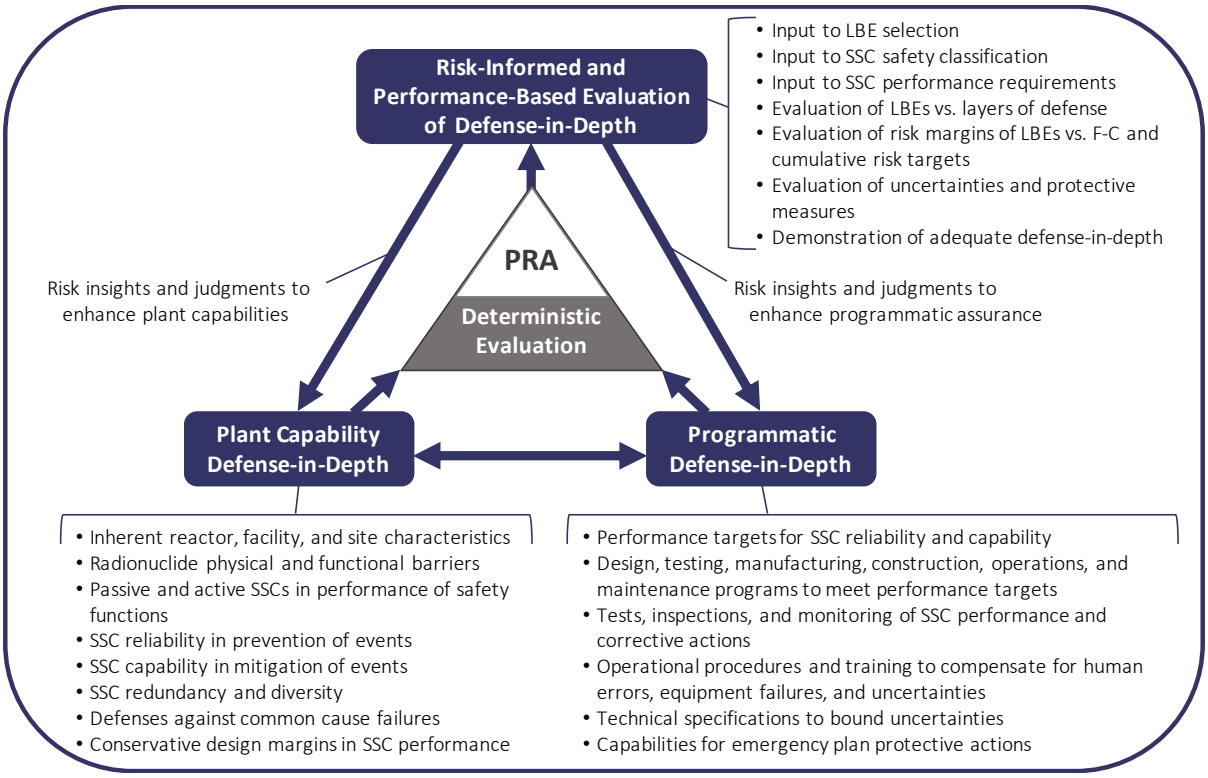

Figure 5-2. Framework for Establishing DID Adequacy

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 unexpected events should they occur. Plant capability DID is divided into the following categories:

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

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

These capabilities, when combined, create layers-of-defense responses to plant challenges.

Programmatic Defense-in-Depth

Programmatic DID is used to address uncertainties when evaluating plant capability DID as well as when programmatic protective strategies are defined. It provides a means to incorporate special treatment* while designing, manufacturing, constructing, operating, maintaining, testing, and inspecting the plant and the associated processes to ensure there is reasonable assurance that the predicted performance

* 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."

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 to 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 (RI) integrated decision-making process to assess sufficiency of DID and to enable consideration of different alternatives for achieving commensurate safety levels at reduced burdens. The outcome of the RI process also establishes a DID baseline for managing risk throughout the plant lifecycle.

The concept of using the layers of defense for performing the RIPB evaluation of plant capabilities and programs, which has been adapted from the IAEA "levels of defense" approach, is shown in Figure 5-3.

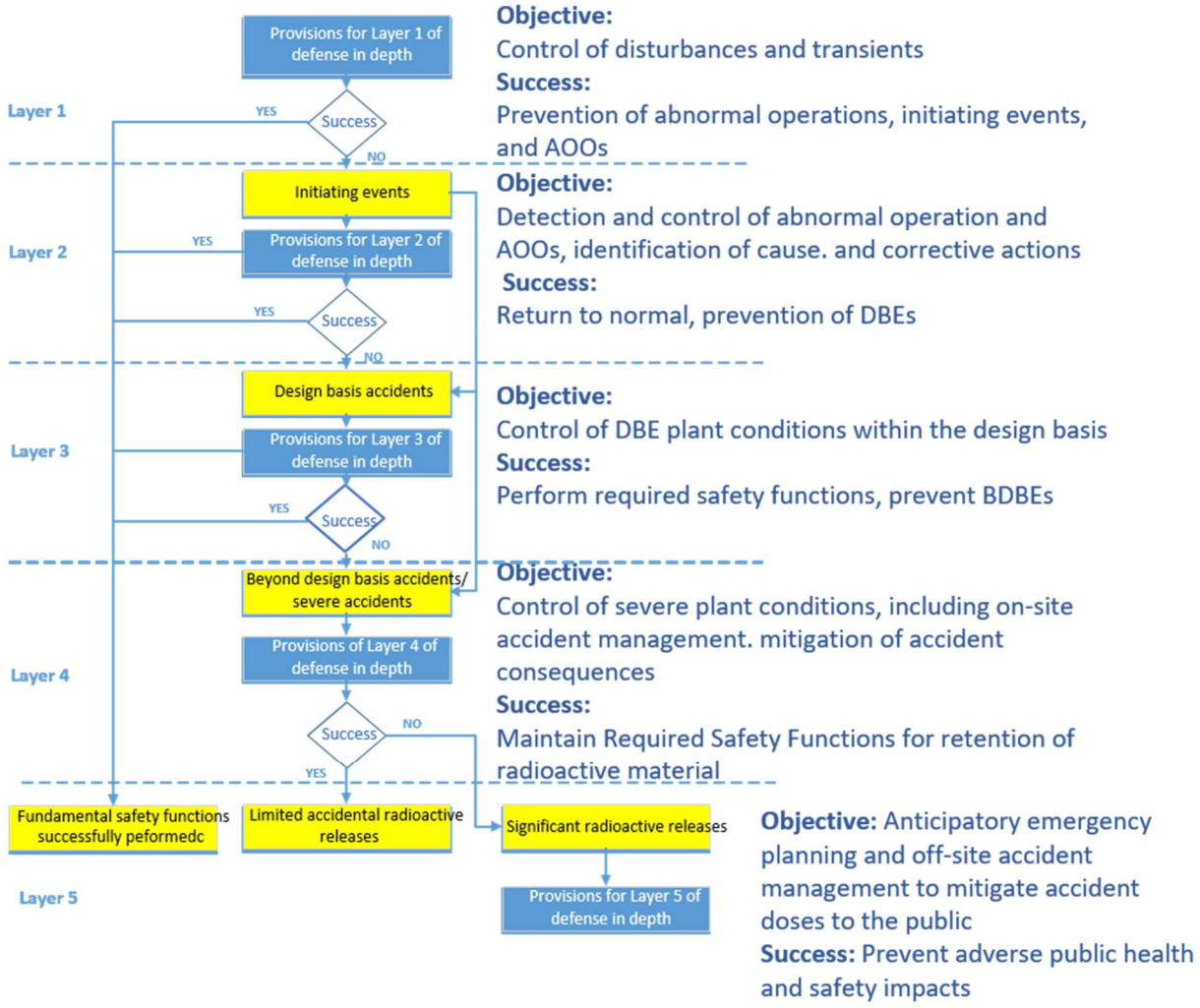

Figure 5-3. Framework for Evaluating LBEs Using Layers of Defense Concept Adapted from IAEA

This framework sets the context to evaluate each LBE and to identify the DID attributes that have been incorporated into the design to prevent and mitigate event 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.

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 indicated 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 process. The DID evaluation includes the identification of compensating protective measures to address the risk-significant sources of uncertainty in both the frequency and consequence estimates.

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-Making Panel (IDP) that guides the overall design effort (including development of plant capability and programmatic DID features), conducts the DID adequacy evaluation of the resulting design, and documents the DID baseline.

The incorporation of DID in each component of this process is illustrated in Figure 5-4, and the key elements of each task in the figure are summarized below. Note that Figure 5-4 includes many actions described previously by this document and does not imply that these steps need to be re-performed for the purpose of the DID adequacy evaluation. The color coding in the figure identifies elements that are probabilistic, deterministic, and risk-informed (i.e., having both probabilistic and deterministic aspects). It is emphasized that the implementation of the process is not a series of discrete tasks but rather an iterative process. As shown by the 'Triangle A' icons in the figure, this iteration is expected to occur repeatedly and at different tasks in the overall process. Iteration through the tasks is expected to continue through the documentation of the DID baseline in Task 18, and then with subsequent DID baseline updates as the design progresses. The sequence of tasks 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.

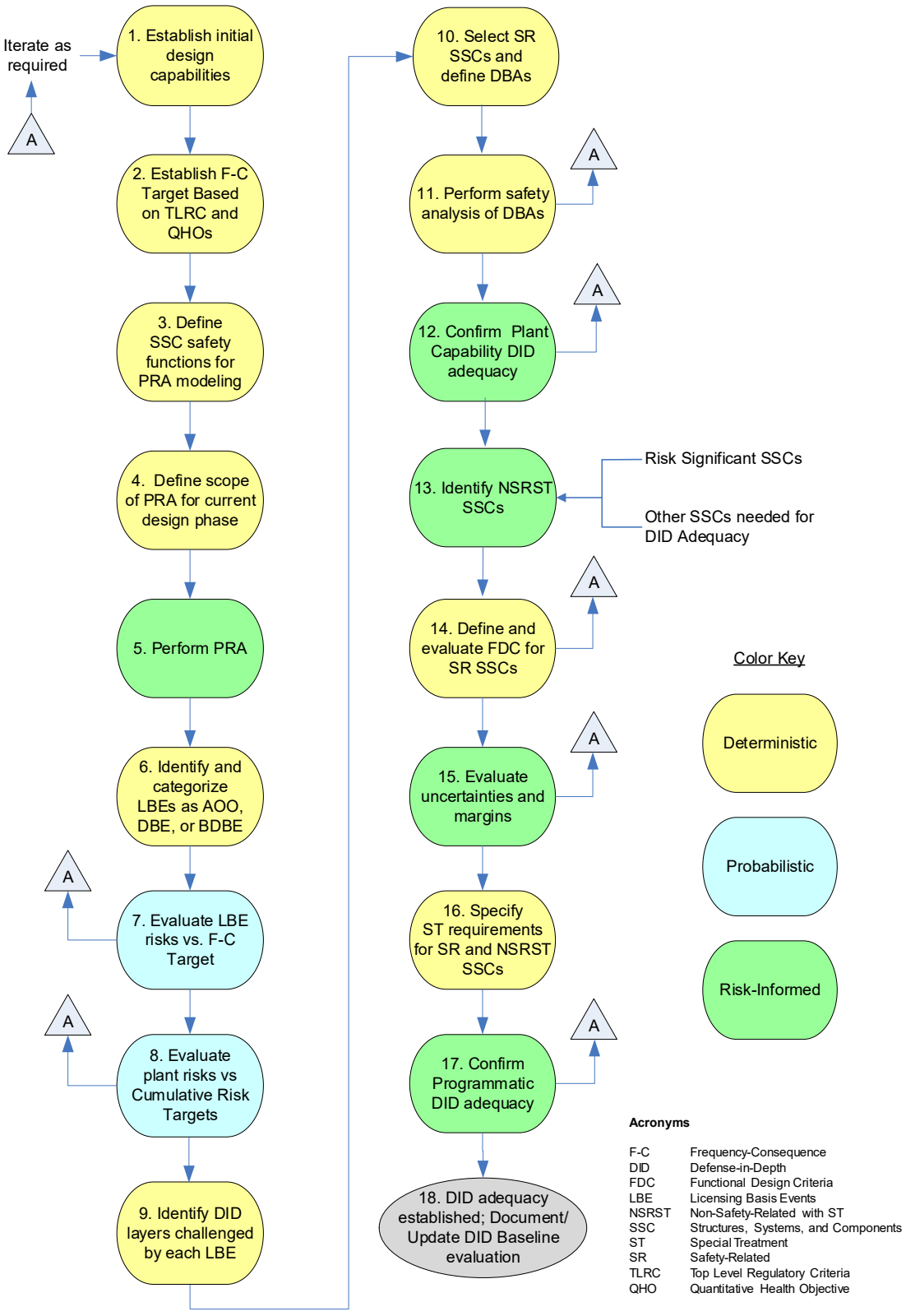

Figure 5-4. Integrated Process for Incorporation and Evaluation of Defense-in-Depth

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

Task 1: Establish Initial Design Capabilities

The process begins in Task 1 with available design information. Top-level requirements are formulated with input from all stakeholders, including 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 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 task include power level, selection of 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 PSFs, supplemented by active systems that provide additional layers of defense to the prevention and mitigation of events, is of particular relevance to any design.

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

* Industry has developed procedures and guidelines for the makeup and responsibilities of such panels. These have been found acceptable by NRC in specific licensee 10CFR50.69 programs.

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 design requirements for operability, availability, maintainability, and investment protection features using conventional practices, industry codes and standards, etc. It is noted that additional plant capabilities as well as programs and compensating measures may be added as a result of maturing probabilistic and deterministic evaluations of plant safety and DID in subsequent tasks.

Initially, the designer makes decisions on both the design and selection of codes and standards that influence design and some baseline level of special treatment. For example, the designer may select certain parts of 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 Task 14. The full extent of special treatment is defined following the evaluation of LBEs and the selection of SSC safety classes for each SSC. Hence, selection of codes and standards supports both the plant capabilities for DID and the activities that contribute to the programmatic DID.

As noted previously, establishing DID capabilities in the plant design is an iterative process. Some portions of the design, such as the reactor island, normally advance earlier than others, like 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.

Task 2: Establish F-C Target Based on Regulatory Objectives and QHOs

The F-C Target derived from regulatory objectives is an important risk-informed element of this process, as discussed previously. The evaluation of DID adequacy in Tasks 12 and 17 focuses on the LBEs and associated SSCs with the highest levels of risk significance.

Task 3: Define SSC Safety Functions for PRA Modeling

The plant designer defines the reactor-specific PSFs in Task 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 PSFs that achieve the FSFs. During this process, the designer confirms the allocation of these safety functions to both passive and active SSCs. The top-level design criteria are also confirmed for all the SSCs selected to perform the reactor-specific safety functions. As Task 3 is completed, the plant capabilities that support DID are largely determined. Adjustments may be made to address the results of subsequent evaluations or design iterations that may expose weaknesses in design or operating assumptions or expose margin or other uncertainties that are relevant to demonstrate adequate levels of safety and sufficient DID.

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

Task 4: Define Scope of PRA for Current Design Phase

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

Task 5: Perform PRA

The performance of the current phase of the PRA is covered in this task consistent with the process described elsewhere in this guidance document. Information from the PRA is used together with deterministic inputs to establish DID adequacy as part of the RIPB evaluation of DID depicted in Tasks 12 and 17. 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 process. The DID evaluation includes the identification of compensating protective measures to address the risk-significant sources of uncertainty in both LBE frequencies and consequences.

Task 6: Identify and Categorize LBEs as AOOs, DBEs, or BDBEs

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

Task 7: Evaluate LBE Risks vs. F-C Target

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

Task 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.

Task 9: Identify DID Layers Challenged by Each LBE

The layers of defense process in Figure 5-3 are used in this task to evaluate each LBE with more attention given 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.

Task 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 by performing sensitivity analyses to determine which of the PSFs modeled in these LBEs are necessary 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 RSFs. In general, there may be two or more different sets of SSCs that could provide these RSFs. Those functions specified by the design team (represented on the IDP) select which of the available SSCs that can support the RSFs for all the DBEs and high-consequence BDBEs are designated as SR. DBAs are then constructed, starting with each

DBE, and then assuming that only the SR SSCs perform their prevention or mitigation function. DID considerations are taken into account in the selection of SR SSCs by selecting those that yield high confidence in performing their functions with sufficient reliability to minimize uncertainties.

Task 11: Perform Safety Analysis of DBAs

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

Task 12: Confirm Plant Capability DID Adequacy

At this task, there is sufficient information, even during the conceptual engineering phase, to evaluate the adequacy of the plant capabilities for DID using information from the previous tasks and guidelines for establishing the DID adequacy. This task is supported by the results of the systematic evaluation of LBEs using the layers of defense process in Task 9. As part of the DID adequacy evaluation, each LBE is evaluated to confirm that risk targets are met without exclusive reliance on a single element of design, a single program, or a single DID attribute.

Task 13: Identify Non-Safety-Related with Special Treatment 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 necessary for DID adequacy. Criteria for classifying SSCs as safety-significant based on DID considerations are 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.

Task 14: Define and Evaluate Required Functional Design Criteria for SR SSCs

RFDC 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 RSFs are used in the formulation of RFDCs.

Task 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 frequencies and consequence as well as other uncertainties which are not sufficiently characterized for uncertainty quantification nor amenable to sensitivity analyses. The plant capability DID includes design margins that protect against uncertainties. The layers of defense within a design, including offsite response, are used to compensate for residual unknowns. The approach to identifying and evaluating uncertainties that are quantified in the PRA and used to establish protective measures reflected in the plant capability and programmatic elements of DID was described previously.

Task 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 PSFs with significant margins and with appropriate degrees of reliability. These include numerical targets for SSC reliability and availability, design margins for performance of the PSFs, and monitoring of performance against these targets with appropriate corrective actions when targets are not fully realized. Another consideration in the setting of SSC performance requirements is the need to assure that the results of the plant capability DID evaluation in Task 12 are achieved not just in the design, but in the as-built and as-operated and maintained plant throughout 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, further special treatments may be identified.

Task 17: Confirm Programmatic DID Adequacy

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

Task 18: DID Adequacy Established; Document/Update DID Baseline Evaluation

The RIPB evaluation of DID adequacy continues until the recurring evaluation of plant and programmatic DID associated with design and PRA update cycles no longer identifies risk-significant vulnerabilities where potential compensatory actions can make a practical, significant improvement to the LBE risk profiles or risk significant reductions in the level of uncertainty in characterizing the LBE frequencies and consequences. At this point, a DID baseline can be finalized to support the final design and operations the plant.

The successful outcomes of Tasks 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 Table 5-1, there are important DID roles in each major element of the process. The IDP uses information and insights in each of these elements to support a risk-informed and performance-based evaluation of DID adequacy. As indicated in Figure 5-2, RIPB decisions that are made in this evaluation feed back any necessary changes to the DID attributes reflected in the plant capability and programmatic elements of DID.

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 event sequences for inclusion into the PRA Selection of passive and active SSCs to perform safety functions with consideration of the NRC Advanced Reactor Safety Policy to simplify designs and rely more on inherent and passive means to fulfill PRA Safety Functions Initial selection of DID attributes for plant capability and programmatic DID
Reactor-Specific PRA	Identification of challenges to each layer of DID and evaluation of the plant responses to them Identification of challenges to physical and functional barriers within layers of defense Characterization of the plant responses to IEs and identification of end states involving successful mitigation and associated success criteria, and unsuccessful mitigation with release of radioactive material from one or more reactor modules or radionuclide sources Assessment of the effectiveness of barriers in retaining fission products via mechanistic source term development and assessment of offsite radiological consequences Assessment of IE frequencies, reliabilities, and availabilities of SSCs necessary to respond to those IEs Identification of dependencies and interactions among SSCs; evaluation of the layers of defense against common-cause failures and functional independence Grouping of event sequences into LBEs based on similarity of IE challenge, plant response, and end state Information for the evaluation of risk significance Identification of risk-significant 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 RSFs Input to the selection of SR SSCs Input to the formulation of conservative assumptions for the deterministic safety analysis of DBAs
SSC Safety Classification and Performance Requirements	Classification of NSRST and NST SSCs Selection of SSC Required Functional Design Criteria Selection of design requirements for SR SSCs Selection of PB 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 SR 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

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 process 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 frequencies and consequences. 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 process for establishing plant capability DID begins in the development of the safety design approach and is accomplished in the course of the iterative process tasks leading up the selection and evaluation of LBEs. It is also impacted by SSC safety classification. Task 7e represents the task in the LBE evaluation in which 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 process, a set of DID adequacy guidelines has been provided. The guidelines, presented in Table 5-2, can be used as a basis for initially evaluating the adequacy of plant capability DID and are confirmed during the regulatory review as appropriate and sufficient.

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

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

5.6.2 DID Guidelines for Defining Safety-Significant SSCs

As discussed in Section 4, SSCs are classified as safety-significant if they perform one or more risk-significant functions or are necessary for DID adequacy. The guidelines in Table 5-2 require that two or more independent plant design or operational features be provided to meet the requirements for each LBE. Any SSCs necessary to meet this requirement, 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 SR nor risk-significant, the IDP would classify the SSC as safety-significant and NSRST.

SSCs regarded as safety-significant but 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 DID adequacy.

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, preventing and mitigating the progression of IEs through the availability of independent levels of protection, and achieving sufficient protection of public health and safety through the use of redundant and diverse means. Additionally, the evaluation determines whether any single feature is excessively relied upon to achieve public safety objectives, and if so, identifies options to reduce or eliminate such dependency. The completion of the evaluation supports an appropriate safety design adequacy determination 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 areas included in the 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 event sequences within and beyond the design basis.

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

Attribute	Evaluation Focus
Initiating Event and Event 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 PRA Safety Functions Passive and Active SSCs performing PRA 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 central element of the RIPB evaluation of DID is a systematic review of the LBEs against the layers of defense. This review by the IDP is necessary to evaluate the plant capabilities for DID and to identify any programmatic DID measures that may be necessary for establishing DID adequacy. In meeting its objectives, the review will:

- Confirm that plant capabilities for DID are deployed to prevent and mitigate each LBE at each layer of defense challenged by the LBE.

- Confirm that a balance between event prevention and mitigation is reflected in the layers of defense for risk-significant LBEs.

- Identify the reliability/availability missions of SSCs that perform prevention and mitigation functions along each LBE and confirm that these missions can be accomplished. A reliability/availability mission is the set of requirements related to the performance, reliability, and availability of an SSC function that adequately ensures the accomplishment of its task, as defined by the PRA or deterministic analysis.

- Confirm that adequate technical bases for classifying SSCs as SR or non-safety-related and risk-significant exist and their capabilities to execute the RSFs are defined.

- Confirm that the effectiveness of physical and functional barriers to retain radionuclides in preventing or limiting release is established.

- Review the technical bases for important characteristics of the LBEs with focus on the most risk-significant LBEs, and LBEs with relatively higher consequences.[*] The technical bases for relatively high-frequency LBEs that are found to have little or no release or radiological consequences is also a focus of the review.

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

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 IEs and event sequences. This understanding is the basis for the formulation of the SSC capability requirements for mitigation of the challenges represented in the LBEs as well as the reliability requirements to prevent LBEs with more severe consequences. This understanding is also important in recognizing how the plant capabilities for DID achieve an appropriate balance between event prevention and mitigation across different layers of defense, which permits an examination of the plant capabilities evaluation 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 RIPB evaluation of DID and plant capability DID. The event sequences are part of the risk-informed evaluation of DID, and the roles of SSCs in prevention and mitigation 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.

[*] 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.

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

Standard Elements of Event 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 PRA 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 PRA 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 process for evaluating LBE prevention and mitigation in Table 5-4 is used to define a simple model for estimating the risk of radionuclide release s associated with a specific event sequence, or LBE:

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

where:

R_j = Expected quantity of radioactive material released per plant-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

This section explains 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 values 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 or large early release frequency and the NRC safety goal QHOs.

A more conservative evaluation of margins, similar to the first form mentioned above, uses the 95th percentile upper bound values for both LBE frequency and dose 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-Making Panel Focus in LBE Review

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

- Is the selection of IEs and event sequences reflected in the LBEs sufficiently complete? Are the uncertainties in the estimation of LBE frequency, plant response to events, mechanistic source

terms, and dose well characterized? Are there sources of uncertainty not adequately addressed?

- Have all risk-significant LBEs and SSCs been identified?
- Has the PRA evaluation provided an adequate assessment of "cliff edge effects?"
- Is the technical basis for identifying the RSFs adequate?
- Is the selection of the SR SSCs to perform the RSFs appropriate?
- Have protective measures to manage the risks of multi-reactor module and multi-radiological source event sequences been adequately defined?
- Have protective measures to manage the risks of all risk-significant LBEs been identified, especially those with relatively high consequences?
- Have protective measures to manage the risks for all risk-significant common-cause IEs such as support system faults, internal plant hazards such as fires and floods, and external hazards been identified?
- Is the risk benefit of all assigned protective measures well characterized, e.g., via sensitivity analyses?

If the evaluation identifies unacceptable answers to any of these questions, additional compensatory action would be considered, depending on the risk significance of the LBE. With reference to Figure 5-4, which identifies feedback loops in the process at each evaluation task of the process, the compensatory action can take on different forms, including changes to design and operation, refinements to the PRA, revisions to the selection of LBEs and safety classification of SSCs, and 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 that adequate margins exist between the assessed LBE risks relative to the F-C Target including quantified uncertainties
- Assuring that adequate margins exist between the assessed total plant risks relative to the cumulative risk targets
- Assuring that appropriate targets for SSC reliability and performance capability are reflected in design and operational programs for each LBE

- Providing adequate assurance that the risk, reliability, and performance targets will be met and maintained throughout the life of the plant with adequate consideration of sources of significant uncertainties

Unlike the plant capabilities for DID that can be described in physical terms and are amenable to quantitative evaluation, the programmatic DID adequacy should 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)
Offsite Response	Emergency response capability

The attributes of programmatic DID complement each other and provide overlapping assurance that the desired 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 to determine that the programmatic DID provides reasonable assurance of adequate protection of public health and safety based on the 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

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

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

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

Evaluation Focus	Implementation Strategies	Evaluation Considerations
Compensation for Mechanical Errors	Operational Technical Specifications Allowable Outage Times Part 21 Reporting Maintenance Rule Scope	1. Are all risk-significant LBE limiting condition for operation reflected in plant Operating Technical Specifications? 2. Are Allowable Outage Times in Technical Specifications consistent with assumed functional reliability levels for risk-significant LBEs? 3. Are all risk-significant SSCs properly included in the Maintenance Program?
Compensation for Unknowns (Performance Variability)	Operational Technical Specifications In-Service Monitoring Programs	1. Are the Technical 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 events identified in the PRA? 4. Has the PRA been peer reviewed in accordance with applicable industry standards and regulatory guidance? 5. Are hazards not included in the PRA low risk to the public based on bounding deterministic analysis?
Offsite Response Attribute		
Emergency Response Capability	Layers of Response Strategies Emergency Planning Zone Location Emergency Planning Programs Public Notification Capability	1. Are functional response features appropriately considered in the design and emergency operational response capabilities for severe events as a means of providing additional DID for undefined event conditions? 2. Is the emergency planning zone appropriate for the full set of DBEs and BDBEs identified in the LBE selection process? 3. Is the time sufficient to execute emergency planning protective actions for risk-significant LBEs consistent with the event timelines in the LBEs?

Quality and Reliability

The initial quality of the design is developed through 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 necessary. 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 topic 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 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 should continually keep in mind that errors are possible, equipment can fail, and real events do not always mimic analytical events. For that reason, the three questions of the risk triplet—1) What can go wrong? 2) How likely is it? and 3) What are the consequences?—should become institutionalized as a part of deciding how to manage residual risk and uncertainty. The primary means of addressing these residual risks is through effective Severe Accident Management Programs and effective emergency planning. Siting considerations and emergency planning zone programs take into account the known risks of a plant, siting the plant in less populated areas and incorporating proactive emergency planning programs that ensure precautionary actions are taken well before a serious threat to public health can arise.

Compensation for Unknowns

The layers-of-defense approach utilized in the DID evaluation process includes the need to define protective measures to address unknowns. Feedback from actual operating and maintenance experience to the PRA provides performance-based outcomes that are part of plant monitoring. Periodic PRA updates should incorporate that information into reliability (system or human) estimates

to determine whether significant LBE risks have changed or new events have 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 BDBE and include provision for event management of potential events 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 can support the more efficient implementation of physical design features in a manner that minimizes the scope of programmatic regulatory 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 Severe Accident Management Guidelines
Technical Specifications	Limiting conditions for operation Surveillance testing requirements Allowable outage (completion) times
Plant Construction and Start-Up Programs	Equipment fabrication oversight Construction oversight Factory testing and qualification Start-up testing
Maintenance and Monitoring of SSC Performance Programs	Operation In-service testing In-service inspection Maintenance of SSCs Monitoring of performance against reliability and capability performance indicators
Quality Assurance Program	Inspections and audits Procurement Independent reviews Software verification and validation
Corrective Action Programs	Event trending Cause analysis Closure effectiveness
Independent Oversight and Monitoring Programs	
Equipment Qualification	Seismic qualification Adverse environment qualification Physical protection
Emergency Planning	

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

In this process, an IDP will be responsible for evaluating DID adequacy. For currently operating plants that employ 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 useful 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 tasks 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 the figure.

5.9.2 Risk-Informed and Performance-Based Decision-Making 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 determination of DID adequacy. RIPB-DM plays a central role in designing and evaluating the DID layers of defense and establishing measures associated with each plant capability and programmatic DID attribute.

Table 5-8 lists the integrated decision-making attributes and principal evaluation focus areas included in the RIPB-DM DID evaluation scope to be executed by the IDP. The RIPB-DM 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 the ASME/ANS PRA Standard for Advanced non-LWRs, which includes the requirement for and completion of the appropriate PRA peer review process, is one means for development 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 Performance-Based Targets and Limits
Uncertainty Management	Magnitude and Sources of Uncertainties
Action Refinement	Implementation Practicality and Effectiveness Cost/Risk/Benefit Considerations

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

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

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

Completing the evaluation of the DID adequacy of a design is not a one-time activity. The designer is expected to employ the RIPB-DM process as often as necessary 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 the F-C Target are sufficient.
    - Risk margins against cumulative risk targets are met.
    - The 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 IEs and event sequences is sufficient.
    - Uncertainties in the estimation of LBE frequencies are evaluated.
    - Uncertainties in the plant response to events are evaluated.
    - Uncertainties in the estimation of mechanistic source terms are evaluated.
    - Design margins in plant capabilities are adequate to address residual uncertainties.
  - Special treatment for all SR and NSRST SSCs is sufficient.

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 and thus recurring consideration of the three questions in the risk triplet: 1) What can go wrong? 2) How likely is it? and 3) 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 explicit components 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, 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, analytical methods or input data accuracy should be examined as well. The focus and level of scrutiny should vary among no/low consequence LBEs and higher consequence LBEs according to risk significance.

Sources of Uncertainties

The greatest number of uncertainties exist in the beginning of the design cycle and are resolved systematically 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, and it should determine 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 results 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 on-site risks to personnel or plant performance and those that could pose risks to the public due to significant non-radiological consequences.

Magnitude of Uncertainties

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

Compensatory Action Adequacy

DID adequacy evaluations should include the necessity, scope, and sufficiency of existing design and operational programs being applied to a design or portion of a design. Specific consideration should be given to the RIPB capabilities of each program type to provide meaningful contributions to risk reduction or performance assurance based on the risk significance of SSCs associated with each LBE. Particular attention should be paid to the number of layers of defense that are associated with IEs that can progressively cascade to the point of challenging public safety objectives. 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 BDBEs, the evaluation should take into account both the magnitude of the consequences and the time frame for actions in determining the need for or choice of compensatory actions. Where dose predictions fall below regulatory limits, the availability of programmatic actions to mitigate those events should be considered over more sweeping changes to plant design to eliminate the BDBE 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 in which the DID evaluation leads to changes in the plant design to enhance the plant capability DID or changes to the protective measures reflected in the programmatic DID. Like many other licensing basis topics, changes in physical, functional, operational, or programmatic features require consideration of the potential for reduction of DID before proceeding. This requires that a current baseline for DID be available as a reference for change evaluation. These changes in turn require revisions to the PRA and all the subsequent tasks in the integrated design process. The first complete pass through the integrated design process will require a baseline DID evaluation which completes the actions of the IDP. 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 recorded 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			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 should be derived from the design records, primarily those that verified that the attributes described 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 RIPB-DM 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 that observable attributes of the design demonstrate the conservative principles supporting DID and 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 lifecycle 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. 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 GLOSSARY OF TERMS

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

LMP Term	Acronym	Definition	Source
Design Basis Event	DBE	Infrequent event sequences that are not expected to occur in the life of a nuclear power plant, which may include one or more reactor modules, but are less likely than AOOs. Event sequences with mean frequencies of 1×10^{-4}/plant-year to 1×10^{-2}/plant-year are classified as DBEs. DBEs take into account the expected response of all SSCs within the plant regardless of safety classification. The objective and scope of DBEs form the safety design basis of the plant.	LMP
Beyond Design Basis Event	BDBE	Rare event sequences that are not expected to occur in the life of a nuclear power plant, which may include one or more reactor modules, but are less likely than a DBE. Event sequences with frequencies of 5×10^{-7}/plant-year to 1×10^{-4}/plant -year are classified as BDBEs. BDBEs take into account the expected response of all SSCs within the plant regardless of safety classification.	LMP
Design Basis Accident	DBA	Postulated accidents that are used to set design criteria and performance objectives for the design of Safety-Related SSCs. DBAs are derived from DBEs based on the capabilities and reliabilities of Safety-Related SSCs needed to mitigate and prevent accidents, respectively. DBAs are derived from the DBEs by prescriptively assuming that only SR SSCs classified are available to mitigate postulated accident consequences to within the 10 CFR 50.34 dose limits.	LMP
Licensing Basis Event	LBE	The entire collection of event sequences considered in the design and licensing basis of the plant, which may include one or more reactor modules. LBEs include normal operation, AOOs, DBEs, BDBEs, and DBAs.	LMP
Frequency-Consequence Target	F-C Target	A target line on a frequency-consequence chart that is used to evaluate the risk significance of LBEs and to evaluate risk margins that contribute to evidence of adequate defense-in-depth	LMP
Risk-Significant LBE	--	An LBE whose frequency and consequence meet a specified risk significance criterion. In the LMP framework, an AOO, DBE, or BDBE is regarded as risk-significant if the combination of the upper bound (95%tile) estimates of the frequency and consequence of the LBE are within 1% of the F-C Target AND the upper bound 30-day TEDE dose at the EAB exceeds 25 mrem.	LMP
Terms Associated with Plant Design and Structures, Systems, and Components			
Design Basis External Hazard Level	DBEHL	A design specification of the level of severity or intensity of an external hazard for which the Safety-Related SSCs are designed to withstand with no adverse impact on their capability to perform their RSFs	LMP
Plant		The collection of site, buildings, radionuclide sources, and SSCs seeking a single design certification or one or more operating licenses under the LMP framework. The plant	LMP

LMP Term	Acronym	Definition	Source
		may include a single reactor unit or multiple reactor modules as well as non-reactor radionuclide sources.	
Multi-Reactor Module Plant	--	A plant comprising multiple reactor modules that are designed and constructed using a modular design approach. Modular design means a nuclear power plant that consists of two or more essentially identical nuclear reactors (modules) and each reactor module is a separate nuclear reactor capable of being operated independent of the state of completion or operating condition of any other reactor module co-located on the same site, even though the nuclear power plant may have some shared or common systems.	Multi-module plant adapted from ASME/ANS-Ra-S-1.4-2013, modular design from 10CFR52.1
Safety-Related SSCs	SR SSCs	SSCs that are credited in the fulfillment of RSFs and are capable to perform their RSFs in response to any Design Basis External Hazard Level	LMP
Non-Safety-Related with Special Treatment SSCs	NSRST SSCs	Non-safety-related SSCs that perform risk-significant functions or perform functions that are necessary for defense-in-depth adequacy	LMP
Non-Safety-Related with No Special Treatment SSCs	NST SSCs	All SSCs within a plant that are neither Safety-Related SSCs nor Non-Safety-Related SSCs with Special Treatment SSCs.	LMP
Risk-Significant SSC	--	An SSC that meets defined risk significance criteria. In the LMP framework, an SSC is regarded as risk-significant if its PRA Safety Function is: a) required to keep one or more LBEs inside the F-C Target based on mean frequencies and consequences; or b) if the total frequency LBEs that involve failure of the SSC PRA Safety Function contributes at least 1% to any of the LMP cumulative risk targets. The LMP cumulative risk targets include: (i) maintaining the frequency of exceeding 100 mrem to less than 1/plant-year; (ii) meeting the NRC safety goal QHO for individual risk of early fatality; and (iii) meeting the NRC safety goal QHO for individual risk of latent cancer fatality.	LMP
Safety-Significant SSC	--	An SSC that performs a function whose performance is necessary to achieve adequate defense-in-depth or is classified as Risk-Significant (see Risk-Significant SSC).	LMP
Safety Design Approach	--	The strategies that are implemented in the design of a nuclear power plant that are intended to support safe operation of the plant and control the risks associated with unplanned releases of radioactive material and protection of the public and plant workers. These strategies normally include the use of robust barriers, multiple layers of defense, redundancy, and diversity, and the use of inherent and passive design features to perform safety functions.	LMP

LMP Term	Acronym	Definition	Source
Terms Associated with Risk-Informed and Performance-Based Regulation and Decision-Making			
Defense-in-Depth	DID	"An approach to designing and operating nuclear facilities that prevents and mitigates accidents that release radiation or hazardous materials. The key is creating multiple independent and redundant layers of defense to compensate for potential human and mechanical failures so that no single layer, no matter how robust, is exclusively relied upon. Defense-in-depth includes the use of access controls, physical barriers, redundant and diverse key safety functions, and emergency response measures."	NRC Glossary
Layers of Defense	--	Layers of defense are those plant capabilities and programmatic elements that provide, collectively, independent means for the prevention and mitigation of adverse events. The actual layers and number are dependent on the actual source and hazard posing the threat. See Defense-in-Depth.	LMP
Performance-Based	PB	An approach to decision-making that focuses on desired objective, calculable or measurable, observable outcomes, rather than prescriptive processes, techniques, or procedures. Performance-based decisions lead to defined results without specific direction regarding how those results are to be obtained. At the NRC, performance-based regulatory actions focus on identifying performance measures that ensure an adequate safety margin and offer incentives and flexibility for licensees to improve safety without formal regulatory intervention by the agency.	Adapted from NRC Glossary definition of performance-based regulation in order to apply to both design decisions and regulatory decision-making
Risk-Informed	RI	An approach to decision-making in which insights from probabilistic risk assessments are considered with other sources of insights	Adapted from NRC Glossary definition of performance-based regulation in order to apply to both design decisions and regulatory decision-making
Risk-Informed and Performance-Based Integrated Decision-Making	RIPB-DM	The union of risk information and performance information to achieve performance-based objectives	
Terms Associated with Probabilistic Risk Assessment			
Initiating Event	IE	A perturbation to the plant during a plant operating state (POS) that challenges plant control and safety systems whose failure could potentially lead to an undesirable end	ASME/ANS-Ra-S-1.4-2013

LMP Term	Acronym	Definition	Source
		state and/or radioactive material release. An Initiating Event could degrade the reliability of a normally operating system, cause a standby mitigating system to be challenged, or require that the plant operators respond in order to mitigate the event or to limit the extent of plant damage caused by the Initiating Event. These events include human-caused perturbations and failure of equipment from either internal plant causes (such as hardware faults, floods, or fires) or external plant causes (such as earthquakes or high winds). An Initiating Event is defined in terms of the change in plant status that results in a condition requiring shutdown or a reactor trip (e.g., loss of main feedwater system, small reactor coolant pressure boundary [RCPB] breach) when the plant is at power, or the loss of a key safety function (e.g., decay heat removal system) for non-power modes of operation. A specific type of Initiating Event may be identified as originating from a specific cause as defined in terms such as "flood-induced transient" or "seismically-induced RCPB breach."	
Event Sequence	ES	A representation of a scenario in terms of an Initiating Event defined for a set of initial plant conditions (characterized by a specified POS) followed by a sequence of system, safety function, and operator failures or successes, with sequence termination with a specified end state (e.g., prevention of release of radioactive material or release in one of the reactor-specific release categories. An event sequence may contain many unique variations of events (minimal cut sets) that are similar in terms of how they impact the performance of safety functions along the event sequence.	ASME/ANS-Ra-S-1.4-2013
Event Sequence Family	-	A grouping of event sequences with a common or similar POS, Initiating Event, hazard group, challenges to the plant safety functions, response of the plant in the performance of each safety function, response of each radionuclide transport barrier, and end state. An event sequence family may involve a single event sequence or several event sequences grouped together. Each release category may include one or more event sequence families. Event sequence families are not required to be explicitly modeled in a PRA. Each event sequence family involving a release is associated with one and only one release category.	
End State		The set of conditions at the end of an Event Sequence that characterizes the impact of the sequence on the plant or the environment. In most PRAs, end states typically include success states (i.e., those states with negligible impact) and Release Categories.	ASME/ANS-Ra-S-1.4-2013
PRA Technical Adequacy	--	A set of attributes that define the technical suitability of a PRA capability to provide fit-for-purpose insights to risk-informed decision-making. It includes consideration of realism, completeness, transparency, PRA model-to-plant as-designed and as-built fidelity state, and identification and evaluation of uncertainties relative to risk levels.	LMP

LMP Term	Acronym	Definition	Source
		Strategies to achieve technical adequacy include conformance to consensus PRA standards, performance of PRA peer reviews, and structured processes for PRA model configuration control, maintenance and updates, and incorporation of new evidence that comprises the state of knowledge reflected in the PRA model development and its quantification.	
Plant Operating State	POS	A standard arrangement of the plant during which the plant conditions are relatively constant, are modeled as constant, and are distinct from other configurations in ways that impact risk. POS is a basic modeling device used for a phased-mission risk assessment that discretizes the plant conditions for specific phases of an LPSD evolution. Examples of such plant conditions include core decay heat level, primary coolant level, primary temperature, primary vent status, reactor building status, and decay heat removal mechanisms. Examples of risk impacts that are dependent on POS definition include the selection of Initiating Events, Initiating Event frequencies, definition of accident sequences, success criteria, and accident sequence quantification.	ASME/ANS-Ra-S-1.4-2013
Mechanistic Source Term	MST	A source term that is calculated using models and supporting scientific data that simulate the physical and chemical processes that describe the radionuclide inventories and the time-dependent radionuclide transport mechanisms that are necessary and sufficient to predict the source term.	ASME/ANS-Ra-S-1.4-2013