Proposal to Establish a Risk-Informed and Performance Based Approach for Event Selection and Component Safety Classification

June 12, 2020

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS

AOO*	anticipated operational occurrence
BDBE*	beyond design basis event
DBA*	design basis accident
DBE*	design basis event
DID*	defense-in-depth
EAB	exclusion area boundary
F-C*	frequency-consequence
FMEA	failure modes and effects analysis
GIF	Generation-IV International Forum
HAZOP	hazard and operability study
HLRC	high level regulatory criteria
IAEA	International Atomic Energy Agency
IE*	initiating event
LBE*	licensing basis event
LWRS	light water reactors
NRC	Nuclear Regulatory Commission
NSRST*	non-safety-related with special treatment
NST*	non-safety-related with no special treatment
PRA	probabilistic risk assessment
QHO	quantitative health objective
RI*	risk-informed
RIPB	risk-informed and performance-based
RSF*	required safety function
RSWG	Risk and Safety Working Group of GIF
SR*	safety-related

SSC	structures, systems, and components
ST	special treatment
TI-RIPB	technology-inclusive, risk-informed, and performance-based
WGSAR	Working Group on the Safety of Advanced Reactors of OECD's CNRA

* 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 Generation IV reactors. This guidance provides a method for establishing the aforementioned topics as part of demonstrating a specific design provides reasonable assurance of adequate radiological protection to the public.

1.2 Background

The development of a technology-inclusive risk-informed and performance-based approach for selection of LBEs and safety classification of SSCs is proposed to address the key Gen-IV reactor development and licensing issues. The proposed approach provides a foundation on which the technology or system-specific efforts on the development of safety design criteria and guidelines are based. The implementation of the process description established through this effort is intended to maintain alignment of the Gen-IV concepts with the multiple levels of defense currently reflected in various international standards (i.e., International Atomic Energy Agency [IAEA], Western European Nuclear Regulators Association [WENRA], Committee on Nuclear Regulatory Activities [CNRA], etc.), while allowing flexibility for advanced reactor concepts to take full advantage of their passive and inherent safety attributes.

The fundamental objective of the safety approach is to provide a technology-neutral approach that can be used by designers, operating organizations and regulators in the design, construction, operation and safety assessment of innovative reactors to ensure nuclear safety. The approach summarized in this report proposes a method for assessing and confirming whether the safety design has met its purpose. The main characteristics of the safety approach should be that it is:

- **Risk-informed:** An approach should be used that combines both deterministic and probabilistic information into the decision-making process in a complementary manner
- **Performance-based**: Where justified, the safety approach, technical bases, and safety requirements should be goal setting and performance based to the extent practical, rather than being prescriptive.

It is noted that the approach described in this paper does not exempt any reactor designer from existing regulations, nor does the process address all regulations applicable to nuclear power plants. Rather, the approach informs the safety design approach which can then be applied to demonstrate compliance with the regulations applicable to a reactor design. In particular, this approach is intended to assist reactor developers and regulators in addressing the following foundational 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 they relate to prevention and mitigation of radiological releases within prescribed limits for the protection of public health and safety?
- /Is the philosophy of DID adequately reflected in the design and operation of the facility?

1.3 Objectives

The objectives of this report are to summarize the risk-informed and [performance based approach that can be used tos:

1. Establish the concept of high-level regulatory criteria (HLRC) that can be implemented within each country's existing structure for protecting public health and safety. Summarize the basic event sequence types that must be addressed in design assessments and associated regulatory actions.
2. Summarize linkage among the plant states, plant event sequences, and the five levels of DID adopted by the IAEA and Generation-IV International Forum (GIF).
3. Establish event-sequence evaluation as the approach that allows facility evaluation against the HLRC, including the option for assessing multi-reactor risk.
4. Describe the structure of the frequency-consequence target as the foundation of the proposed approach.
5. Establish a structured risk-informed approach that can be repeatedly applied while achieving consistent results when integrating the use of deterministic inputs and risk insights to identify and categorize events.
6. Describe the conservative and deterministic assumptions applied to derive design-basis accidents (DBAs) from risk-informed design basis events (DBEs).
7. Suggest a lower-frequency cutoff approach for potentially high-consequence event sequences, including the consideration of cliff-edge effects. It is noted that the selected cutoff frequency may be different among member countries.
8. Establish a process to effectively classify SSCs, with the goal of focusing attention and resources on those SSCs that are most risk significant.
9. Describe key constituents of DID, including plant capability and programmatic aspects and their role in evaluating DID adequacy.

1.4 Expected Benefits of the Approach Summarized in this Report

Benefits resulting from the application of this approach are expected to include:

- Provides a technology inclusive process that allows considerations and flexibilities regarding the potentially improved safety margins and innovative design approaches associated with advanced non-light-water reactors (LWRs), while maintaining protection of the public by implementing the concept that safety is "built in rather than added on".
- Establishes an agreed-upon risk-informed and performance-based approach to event sequence categorization and evaluation, providing a foundation that technology developers can implement early in the design process to to better assure a successful regulatory review and efficient facility deployment.
- Establishes a process to classify SSCs and assure that resources are focused on those SSCs that are most risk significant.
- Provides a framework for a transparent and consistent way to assess the adequacy of DID measures, including the concept of practical elimination.

2 LICENSING BASIS DEVELOPMENT PROCESS

This guidance document describes 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 process is:

- 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 intended outcome from executing the processes in this guidance is a risk-informed and performance-based safety basis for the design and developing a safety-focused license application 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 (SFs) modeled in the Probabilistic Risk Assessment (PRA). SFs 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 SFs 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 document is organized as follows to support implementation:

- Section 3 provides a description of the LBE selection and evaluation process.
- Section 4 provides a description of SSC classification process and derivation of performance requirements.
- Section 5 provides a description of the DID adequacy evaluation process.

3 SELECTION OF LICENSING BASIS EVENTS

3.1 High Level Regulatory Criteria

The term HLRC refers to limits on radiological releases for various plant events. The HLRC are:

- Generic, technology-neutral, and independent of plant site
- Quantitative, and thereby useful in a performance-based context
- Direct statements of acceptable consequences or risks to the public

In general, the HLRC are associated with event sequences (i.e., dose at the fence), rather than on initiating events; different event sequences following an initiating event have different frequencies and consequences.

Application of the approach being described in this paper also allows for the assessment of multi-reactor module risk for an entire facility, rather than being limited to an individual reactor basis.

3.2 Licensing Basis Event Definitions

International agencies, design organizations, and regulatory bodies generally all apply a set of specific terms to the various plant states, initiating events, and event sequences that form the bases for a reactor technology's design, safety assessment, and licensing. The definitions in Table 3-1 are intended to establish transparent and consistent description of existing terms, understanding that they will likely need some adjustment to align with past use and current regulatory requirements within each member country.

Table 3-1. Definitions of Licensing Basis Events

Event Type	Guidance Document Definition
Anticipated Operational Occurrences (AOOs)	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. AOOs take into account the expected response of all SSCs within the plant, regardless of safety classification. However, safety grade systems are not relied on to provide an acceptable plant response and outcome from AOO event sequences.
Beyond Design Basis Events (BDBEs)	Very rare event sequences that are not expected to occur in the life of a nuclear reactor fleet, which may include one or more reactor modules or sources, are less likely than a DBE, but are still considered in the design. BDBEs take into account the expected response of all SSCs within the plant regardless of safety classification.
Design Basis Accidents (DBAs)	Postulated event sequences that are less likely than AOOs and not expected to occur in the life of a nuclear power plant, which may include one or more reactor modules or sources, but are considered in the design. DBAs are used to set design criteria and performance objectives for the design of safety-related (SR) SSCs, since DBA response relies on only SR SSCs to mitigate and limit the consequences of postulated event sequences to within the regulatory dose limits for offsite releases.
Design Basis Events (DBEs)	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. DBEs are the basis for the design, construction, and operation of the SSCs during accidents and are used to provide input to the definition of DBAs. DBEs take into account the expected response of all SSCs within the plant regardless of their safety classification.
Licensing Basis Events (LBEs)	The entire collection of event sequences considered in the design and licensing basis of the plant, which includes all radionuclide sources and may include one or more reactor modules. LBEs include AOOs, DBEs, BDBEs, and DBAs.

3.3 Licensing Basis Event Selection Approach

3.3.1 Frequency–Consequence Evaluation Targets

This approach uses a set of frequency–consequence criteria that depict a correlation between the HLRC and targets for evaluating the AOO, DBE, and BDBE event sequence types. This frequency–consequence evaluation correlation, hereafter referred to as the frequency-consequence (F-C) Target, is shown in Figure 3-1.

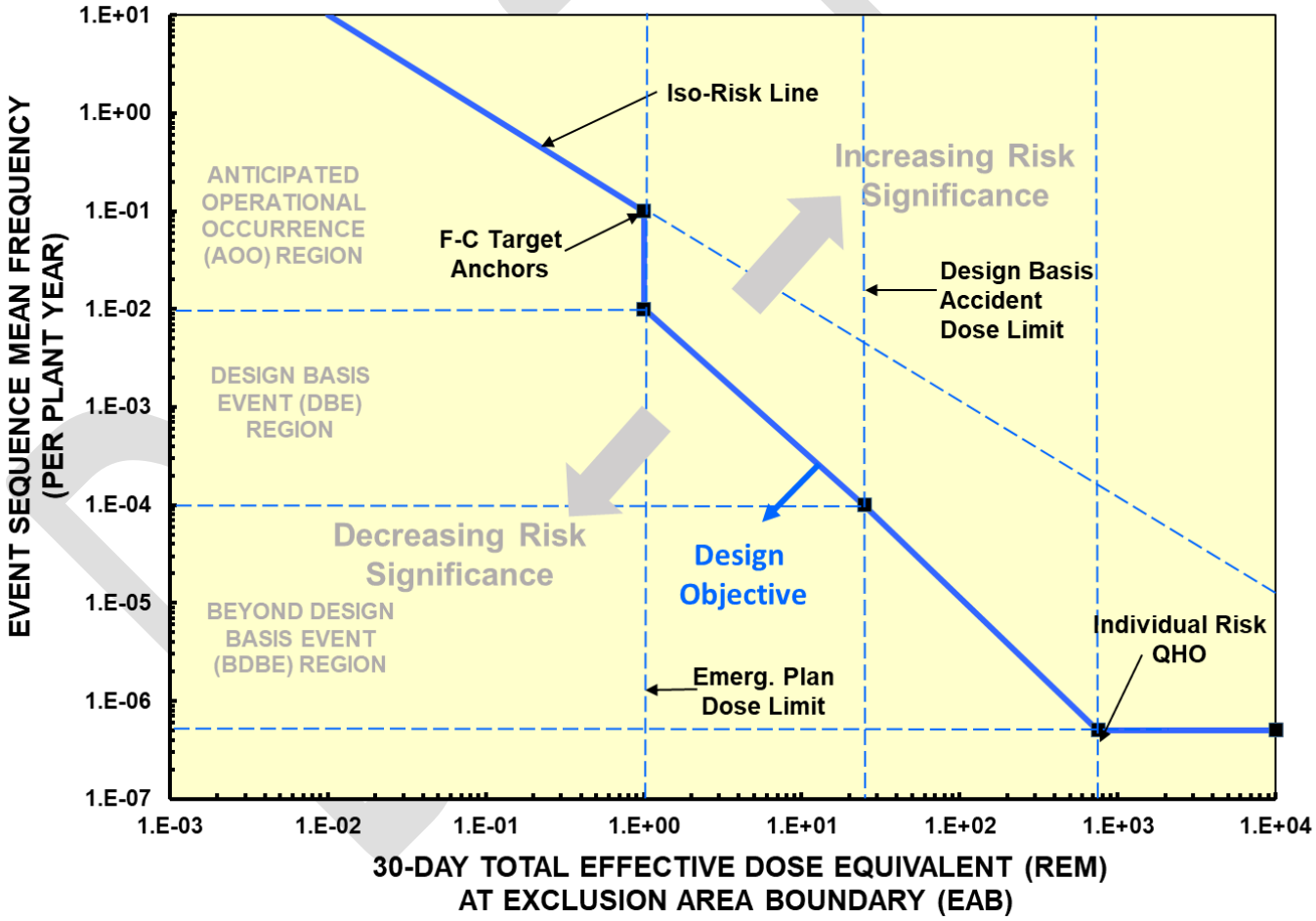

Figure 3-1. Frequency-Consequence Target

The F-C Target in this figure aligns with HLRC in the U.S. and is presented here as an example. It is recognized that the event sequence frequencies and dose limits will vary from country-to-country. However, the overall structure of the F-C Target concept is expected to be applicable and provides a comprehensive and systematic representation of high-level requirements that can be consistently utilized by both designers and regulators. The F-C Target in this figure is based on the following considerations:

- 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 on a site.

- The frequency of event-sequence categories is evaluated on a per-plant-year basis, which allows for event sequences involving multiple reactors and co-located sources within the plant to be evaluated in combination.
- LBE categories are based on mean event sequence frequency of occurrence per plant-year; however, uncertainties about the means are explicitly accounted for.
- The regions of the graph separated by the frequency-dose evaluation line are identified as “Increasing Risk Significance” and “Decreasing Risk Significance” to emphasize that the purpose of the criteria is to evaluate the risk significance of individual AOOs, DBEs, and BDBEs.
- It is expected that many LBEs will not result in the release any radioactive material, although they are still evaluated. The identification of plant capabilities to prevent such releases is a key factor considered in the formulation of SSC safety classification and performance requirements, as discussed more fully in Section 4.
- The F-C Target for the BDBEs range from 25 rem at 10^{-4}/plant-year (example US values) to 750 rem at 5×10^{-7}/plant-year (example US values) to ensure that the quantitative health objective (QHO) for early health effects is not exceeded for individual BDBEs. The question of meeting the QHO for the integrated risks over all the LBEs is addressed using separate cumulative risk targets described later in this guidance document.
- A lower frequency cutoff for potentially high-consequence event sequences is established at 5×10^{7}/plant-year (example US value). 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 DID.
- 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.

3.3.2 **Licensing Basis Event Selection Process**

A logic chart indicating the tasks to identify and evaluate LBEs in concert with the design evolution is shown in

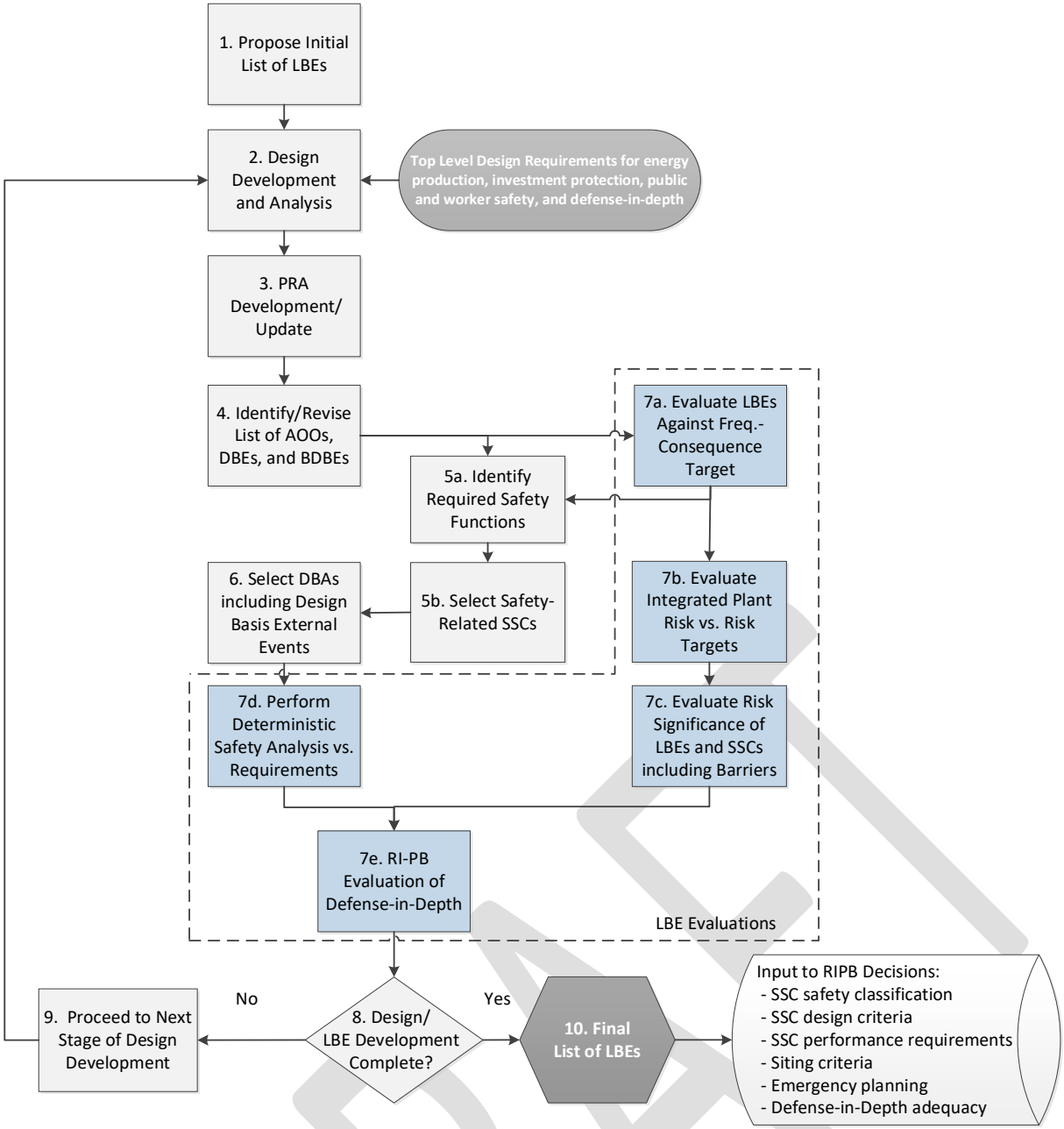

Figure 3-2. The tasks are carried out by the design teams and design evaluation teams responsible for establishing the elements of the safety design and preparing a license application. The LBE selection and evaluation process is implemented in LBE selection tasks described below.

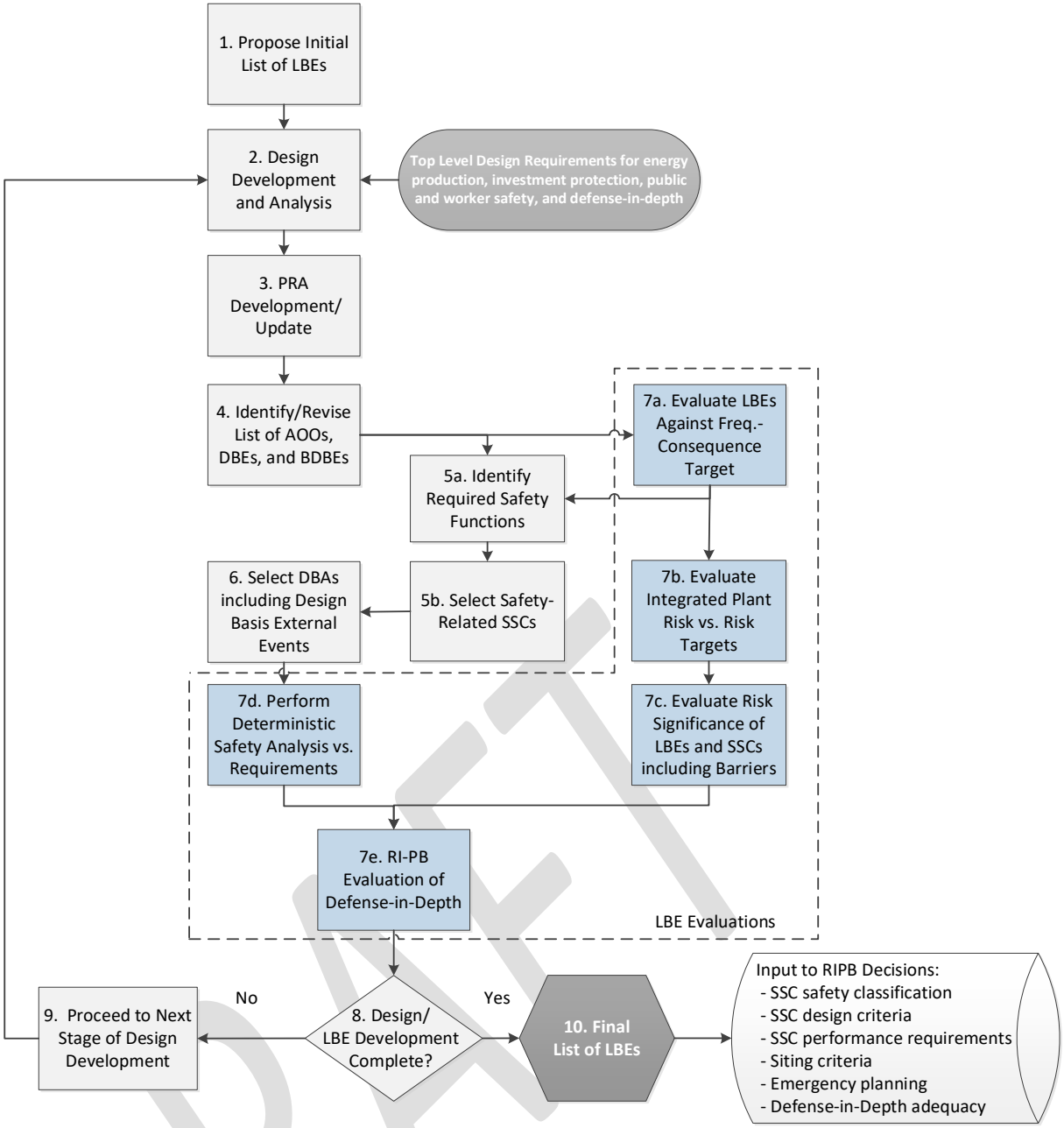

Figure 3-2. Process for Selecting and Evaluating LBEs.

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 similar reactors.

Note: It is recognized that member countries may have requirements for identifying and addressing "practically eliminated situations" (PES). The PES are addressed by the designer by first identifying all plausible single initiating events, as well as a limited number of postulated sequences which might lead to

severe plant conditions and/or specific situations which would lead to large early releases. Within this proposed approach, the resulting LBEs (event sequences) are then evaluated through the following set of tasks to assure that they are appropriately categorized and "dealt with" in a manner that is consistent with the frequency-consequence target. A portion of these event sequences may be shown to have been "practically eliminated" if the assessment of their frequency and consequence places them in the "residual risk" portion of the frequency-consequence figure above. These practically impossible "residual risk" sequences will not be addressed by the design, but will be a consideration when establishing Level 5 of the DID approach.

Task 2: Design Development and Analysis

Design development is performed in phases and often includes a conceptual, preliminary, and final design phases 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. Previously identified technology-neutral safety design considerations and/or technology-specific safety design considerations can be used as inputs. 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 safety-related SSCs that are needed for the deterministic safety analysis in Task 7d.

Task 3: PRA Development/Update

The PRA may be introduced at any stage of design, however the benefits of incorporation of risk insights into the design favor early introduction. 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.

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 includes event sequences involving single or multiple reactor modules and radionuclide sources. This approach provides useful risk insights into the design to ensure that event sequences involving multiple reactor modules are not risk-significant.

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, 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.

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).

Event sequences with upper 95th percentile frequencies less than 5×10^{-7}/plant-year (US value) 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 DID in Task 7e.

Task 5a: Identify Required Safety Functions (RSFs)

In Task 5a, the full set of DBEs are examined to identify the Required Safety Functions (RSFs) that are necessary to conservatively ensure that the acceptable specified offsite dose requirements can be met. The RSFs are responsible for mitigating DBE consequences within the acceptable requirement. For any high-consequence BDBEs, the RSFs are responsible for preventing the event sequences from increasing in frequency into the DBE region by exhibiting sufficient reliability performance. The RSF identification is illustrated conceptually in Figure 3-3with a horizontal arrow for the DBEs and a vertical arrow for the high consequence BDBE.

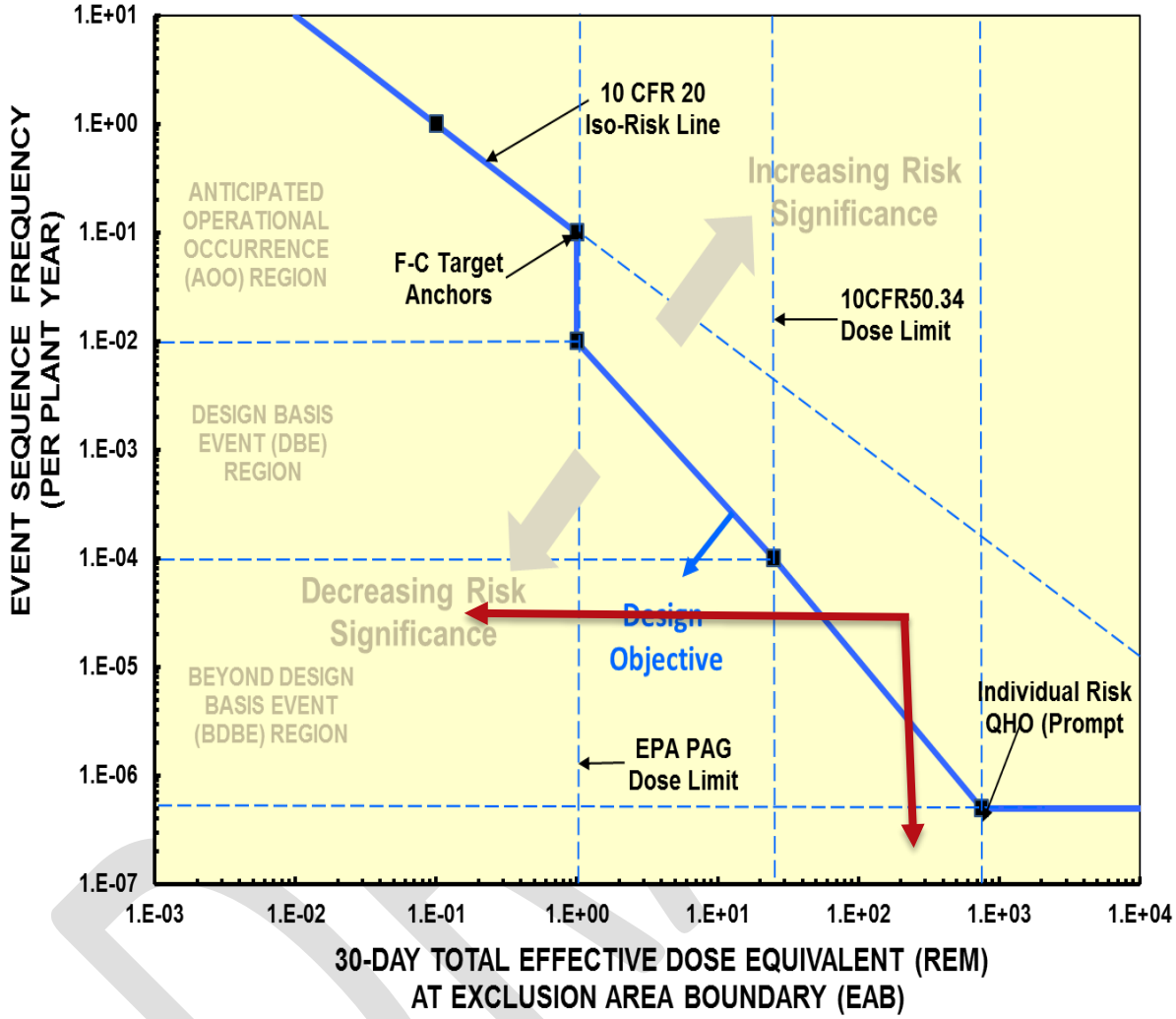

Figure 3-3. Identification of Required Safety Functions Illustrated on F-C Target Figure.

Typical mitigation RSFs for all DBEs are to control reactivity, retain radionuclides, or remove core heat. A typical prevention RSF for high consequence BDBEs might be maintain core geometry.

Task 5b: Select/Revise Safety-Related SSCs

For each of these RSFs identified in Task 5a, one or more SSCs are classified as SR among those found to be available for the spectrum of DBEs. As a result of this selection, each DBE is mitigated by a set of SR SSCs to perform each RSF. Safety related SSCs (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.

Task 6: Select Deterministic DBAs

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, that is, all non-SR SSCs that perform these same functions are assumed to be unavailable. These DBAs are then used in the DBA analysis of the license application for supporting the conservative deterministic safety analysis.

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, rather, it serves as a tool to focus the attention of the designer and those reviewing the design and related operational programs to the most significant events and possible means to address those events.

DBE doses, if any, are evaluated against the F-C Target based on the mean estimates of consequence. This approach is based on the fact that, although the use of a conservative dose evaluation is appropriate for the deterministic safety analysis, it 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.

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 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 of the deterministic DBAs, defined as the 95th percentile of the uncertainty distribution, are required to meet the regulatory dose limits for offsite releases

(US example). Sources of uncertainty in both frequencies and consequences of LBEs are identified and addressed in the approach to evaluate the adequacy of DID.

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 Applicable Regulatory Limits

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

- The total mean frequency of exceeding a site boundary dose limit from all LBEs should not exceed specified limits. 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 average individual risk of early fatality within a specified range of the exclusion area boundary (EAB) from all LBEs based on mean estimates of frequencies and consequences shall not exceed specified limits to ensure that the country's safety goal QHO for early fatality risk is met.
- The average individual risk of latent cancer fatalities within a more extended specified range of the EAB from all LBEs based on mean estimates of frequencies and consequences shall not exceed specified limits to ensure that the country's safety goal QHO for latent cancer fatality risk is met.

The specific numerical limits for each of the three targets above should be tied to each country's regulatory limits and safety goals. In the US application, the first specified limit is 1/plant year to conform to 10 CFR 20; the second is set at $5\times^{-7}$/plant year; and the third to 2×10^{-6}/plant year to conform to the Nuclear Regulatory Commission (NRC) safety goal QHOs.

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 also leads to performance requirements and design criteria that are developed within the process of the SSC classification task.

In addition to the two QHOs, the first cumulative risk target 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 release barriers. In the US, for example, 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

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 with reliance only on SR SSCs.

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

In this task, the definition and evaluation of LBEs is 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.

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.

3.4 Role of the Probabilistic Risk Assessment in Licensing Basis Event Selection

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 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 3-4. 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. 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. Decisions to defer the introduction of the PRA to later stages of the design process lead to reduced opportunities for cost-effective risk management.

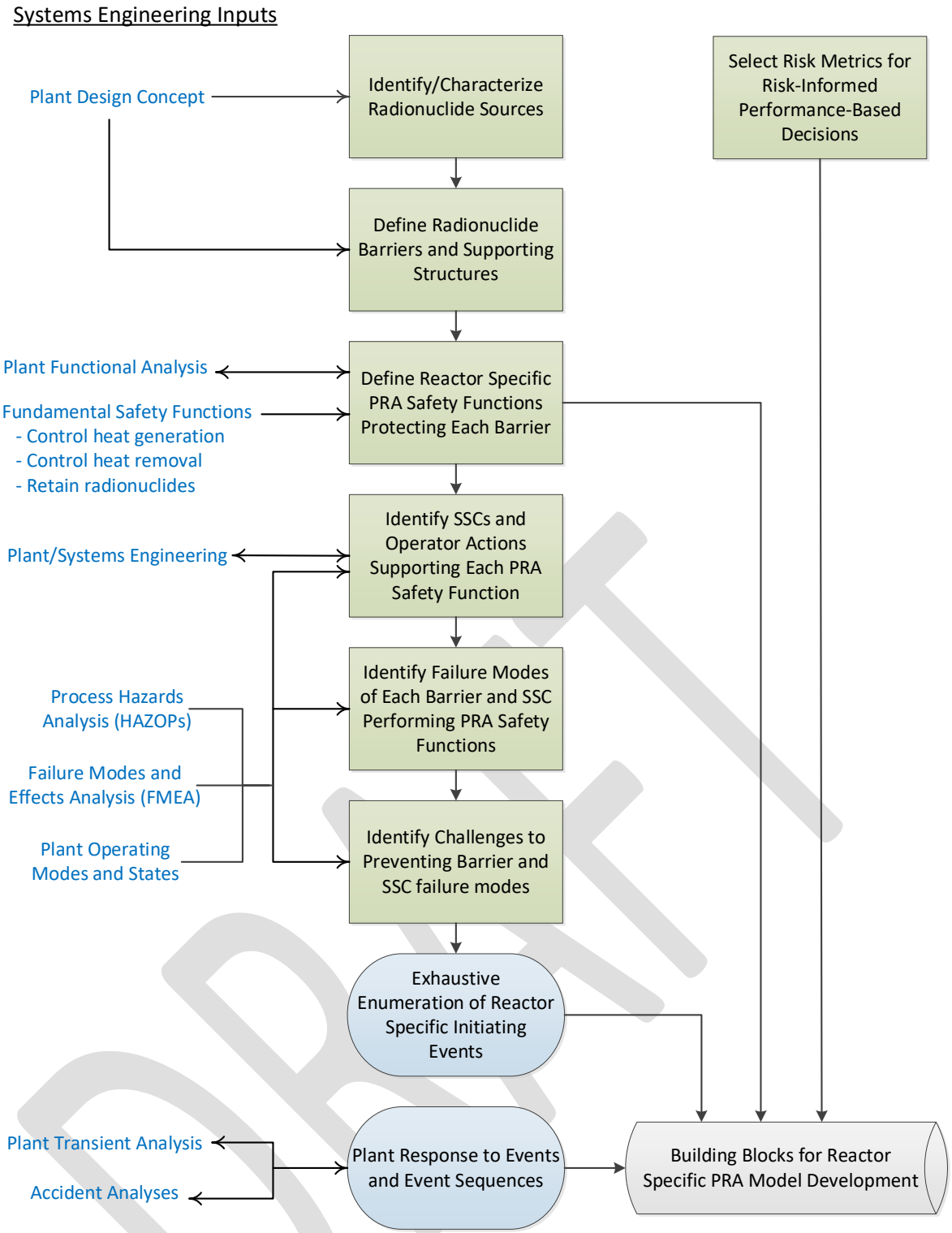

Figure 3-4. Flow Chart for Initial PRA Model Development

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. SSCs that perform the SFs that protect the barriers serve to prevent challenges to the barriers or enhance their effectiveness in preventing or limiting releases of radioactive material.

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 including internal and external events/hazards. The modeled event sequences include the contributions from common-cause failures.

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.

3.4.1 Selection of Risk Metrics for PRA Model Development

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.
- 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.
- Consequences are quantified in terms of offsite radiological effects on the public and environment.

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 SFs in the prevention and mitigation of LBEs that are modeled in the PRA.. Such requirements include those that provide the necessary capabilities to perform their mitigation functions and those that meet their reliability targets to prevent LBEs with more severe consequences.

Two of the classification categories described below incorporate the term “Special Treatment”. 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."

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 regulatory dose limits using conservative assumptions.
  - SSCs selected by the designer and relied on to perform RSFs to prevent the frequency of BDBEs with consequences greater than regulatory dose limits from increasing into the DBE region and beyond the F-C Target.
- Non-Safety-Related with Special Treatment (NSRST):
  - Non-SR 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-SR SSCs relied on to perform functions requiring special treatment for DID adequacy.
- Non-SR with No Special Treatment (NST):
  - All other SSCs (with NST required)

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

4.1 Definition of Safety-Significant and Risk-Significant SSCs

The concepts used to classify SSC functions as risk-significant and safety-significant are illustrated in Figure 4-1, and are further described in Sections 4.1.1 and 4.1.2.

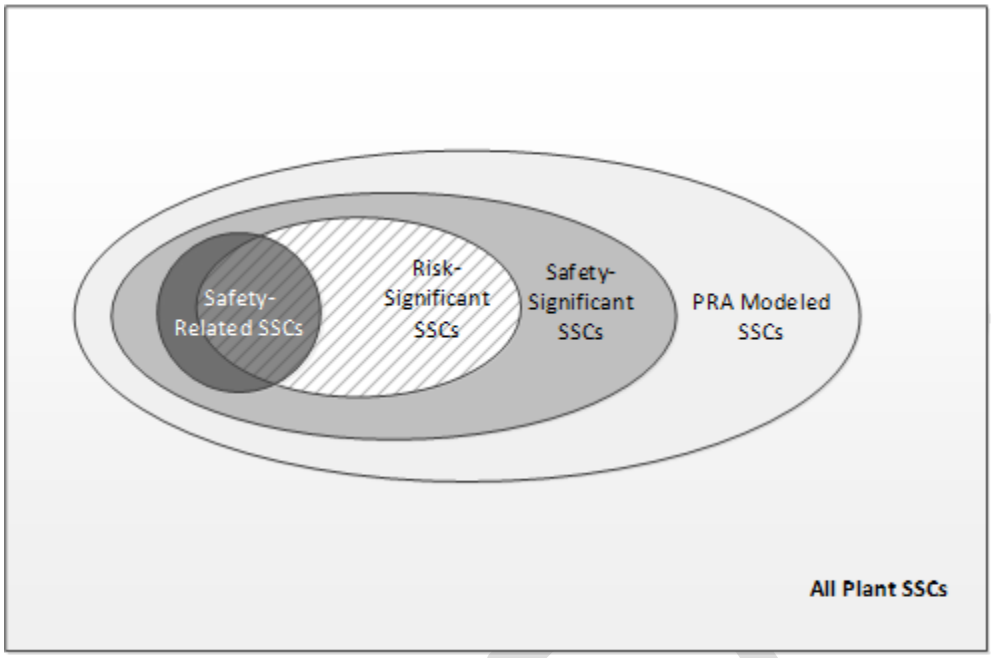

Figure 4-1. Depiction of Safety-Significant and Risk-Significant SSCs

4.1.1 Safety-Significant Structures, Systems, and Components

The meaning of safety-significant SSC in this process is as follows:

> *"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."*

4.1.2 Risk-Significant Structures, Systems, and Components

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. It is also noted that 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 based on the mean estimates of frequencies and consequences. 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, because the F-C Target is only used to evaluate the risk significance of individual LBEs, whereas an SSC may be involved in many LBEs. The cumulative risk metrics and limits include:
  - The total mean frequency of exceeding a site boundary dose should not exceed 1/plant-year to ensure that the annual exposure limits are not exceeded based on the mean estimates of frequencies and consequences. An SSC makes a significant contribution to this cumulative

risk metric if the total frequency of exceeding a site boundary dose associated with LBEs when the SSC has failed is greater than 10^{-2}/plant-year.

- The average individual risk of early fatality within a specified range of the EAB shall not exceed 5×10^{-7}/plant-year based on the mean estimates of frequencies and consequences to ensure that the safety goal QHO for early fatality risk is met (US example). An SSC makes a significant contribution to this cumulative metric if the individual risk of early fatalities associated with the LBEs when the subject SSC has failed is greater than 5×10^{-9}/plant-year.
- The average individual risk of latent cancer fatalities within a more extended specified range of the EAB shall not exceed 2×10^{-6}/plant-year based on the mean estimates of frequencies and consequences to ensure that the safety goal QHO for latent cancer fatality risk is met (US example). An SSC makes a significant contribution to this cumulative risk metric if the individual risk of latent cancer fatalities associated with the LBEs when the subject SSC has failed is greater than a specified frequency limit, such as 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.

4.2 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 the LBE selection and evaluation process is completed in each phase of the design process.

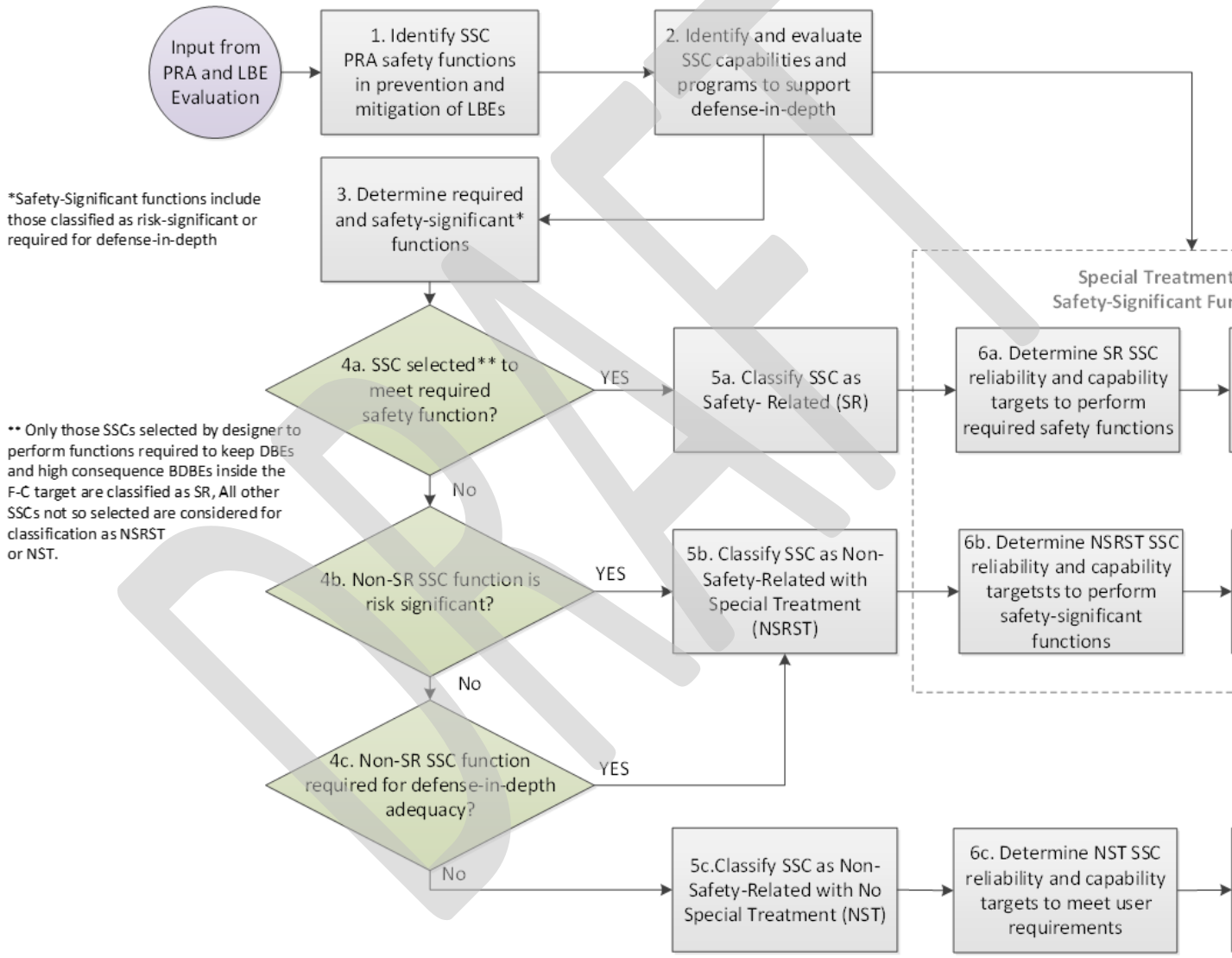

Figure 4-2. SSC Function Safety Classification Process

The SSC safety classification process is implemented in the 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 targets 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 SFs 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 functions regarded as safety-significant. Safety-significant SSCs include those that perform risk-significant functions and those that perform functions that are necessary to meet DID criteria.

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 regulatory limits) are examined to determine which SSCs are available to perform the RSFs. The designer then selects one or more 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 analysis of the DBAs.

Tasks 4B and 5B

In this task, each non-SR 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-SR 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.

Task 6: SSC Reliability and Capability Targets

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.

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.

4.3 Structures, Systems, and Components 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. As a result, safety-significant SSCs include 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.

4.4 Development of Structures, Systems, and Components 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. 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.

4.4.1 Required Functional Design Criteria for Safety-Related Structures, Systems, and Components

As noted previously, SSCs classified as SR perform one or more SFs that are required to perform either of the following:

1. Mitigate DBAs within regulatory dose limits.

2. Prevent any high-consequence BDBEs (those with doses exceeding regulatory dose limits) from exceeding 1×10^{-4}/plant-year (US example) 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 Reactor Functional Design Criteria (RFDCs) from which the safety related design criteria (SRDC) 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 design would require the development of a unique set of RFDCs.

4.4.2 Regulatory Design Requirements for Safety-Related Structures, Systems, and Components

For each of the RFDCs, each designer should identify a set of SRDC 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.

4.4.3 Evaluation of Structures, Systems, and Components 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-SR 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-SR SSCs across the full set of LBEs, including the DBAs.

5 EVALUATION ~~OF~~ DEFENSE-IN-DEPTH ADEQUACY

The philosophy of DID is to provide multiple independent but complimentary means for protecting the public from potential harm from nuclear reactor operation. This evaluation approach provides for the establishment of DID in design, construction, maintenance, and operation of nuclear facilities, and then provides for an objective assessment of DID adequacy. 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.

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 general objectives of this proposed approach are for the evaluation of DID adequacy to be:

- Systematic and Reproducible.
- Sufficiently Complete.
- Available for Timely Input to Design Decisions.
- Risk-Informed and Performance-Based.
- Reactor Technology-Inclusive.

- Compatible with Applicable Regulatory Requirements.

Achievement of DID occurs when all stakeholders (designers, operators, regulators, etc.) implement clear and consistent decisions regarding DID adequacy as an integral part of the overall design and operation.

The three key elements of the approach for establishing and evaluating the adequacy of defense in depth include plant capability DID, programmatic DID, and RIPB evaluation of DID. These three key elements, reflected in the following figure and described below, set 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.

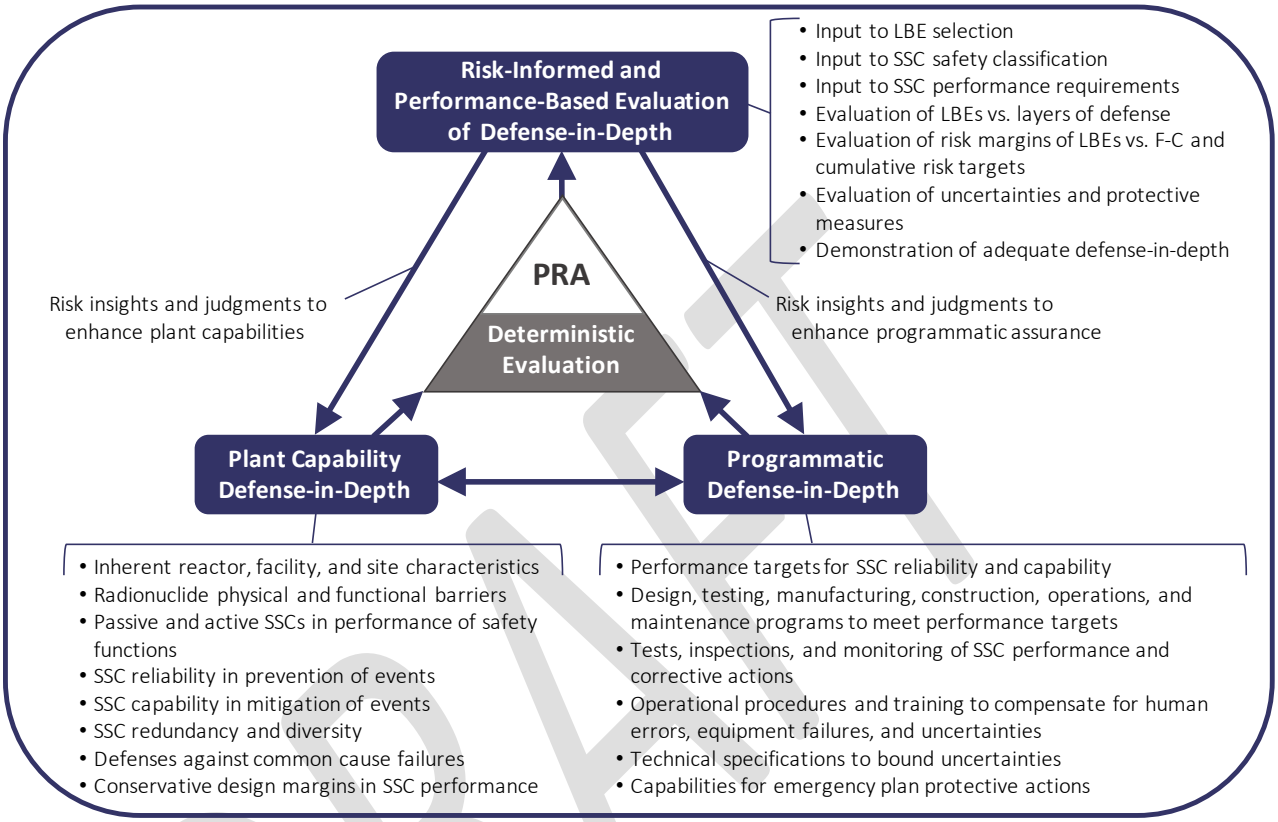

Figure 5-1. Integrated Framework for Incorporation and Evaluation of Establishing DID Adequacy

5.1 Plant Capability Defense-in-Depth

Integrated Framework for Incorporation and Evaluation of DID Adequacy

This element is used by the designer to select functions, SSCs, and their 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.

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 table below provides a listing of the integrated DID attributes and principal evaluation focus of the Plant Capability DID evaluation.

Table 5-1. 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 IEs and transients and thereby contribute to the protective strategies for this layer of DID. Quantitative and qualitative targets for these parameters are design specific.
[c] This criterion implies no excessive reliance on programmatic activities or human actions and that at least two independent means are provided to meet this objective.
[d] The level of margins between the LBE risks and the QHOs provides objective evidence of the plant capabilities for DID. Sufficiency will be decided by the IDP.</td></tr>
</table>

Plant capability DID is deemed to be adequate when:

- Plant capability DID guidelines in adequacy table are satisfied.
- Risk margins against F-C Target are sufficient.
- Risk margins against cumulative risk targets are met.

- Role of SSCs in the prevention and mitigation at each layer of defense challenged by each LBE is understood.
- Prevention/mitigation balance is provided across layers of defense.
- 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.

5.2 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 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 essential.

Programmatic DID includes the following aspects:

- Performance targets for SSC reliability and capability.
- Design, testing, manufacturing, construction, operations, and maintenance programs to meet performance targets.
- Tests, inspections, and monitoring of SSC performance and corrective actions.
- Operational procedures and training to compensate for human errors, equipment failures, and uncertainties.
- Technical specifications to bound uncertainties.
- Capabilities for emergency plan protective actions.

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 5-3.

Table 5-2. 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 Phenomena Identification and Ranking Table (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?

5.3 Risk-Informed Performance-Based 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 risk-informed evaluation is

performed to assess sufficiency of DID and to enable consideration of different alternatives for achieving commensurate safety levels at reduced burdens. The outcome also establishes a DID baseline for managing risk throughout the plant lifecycle.

The concept of using the layers of defense for performing the risk-informed evaluation of plant capabilities and programs, which has been adapted from the IAEA "levels of defense" approach, is shown in Figure 5-2. Those LBEs with the highest levels of risk significance are given greater attention in the evaluation process.

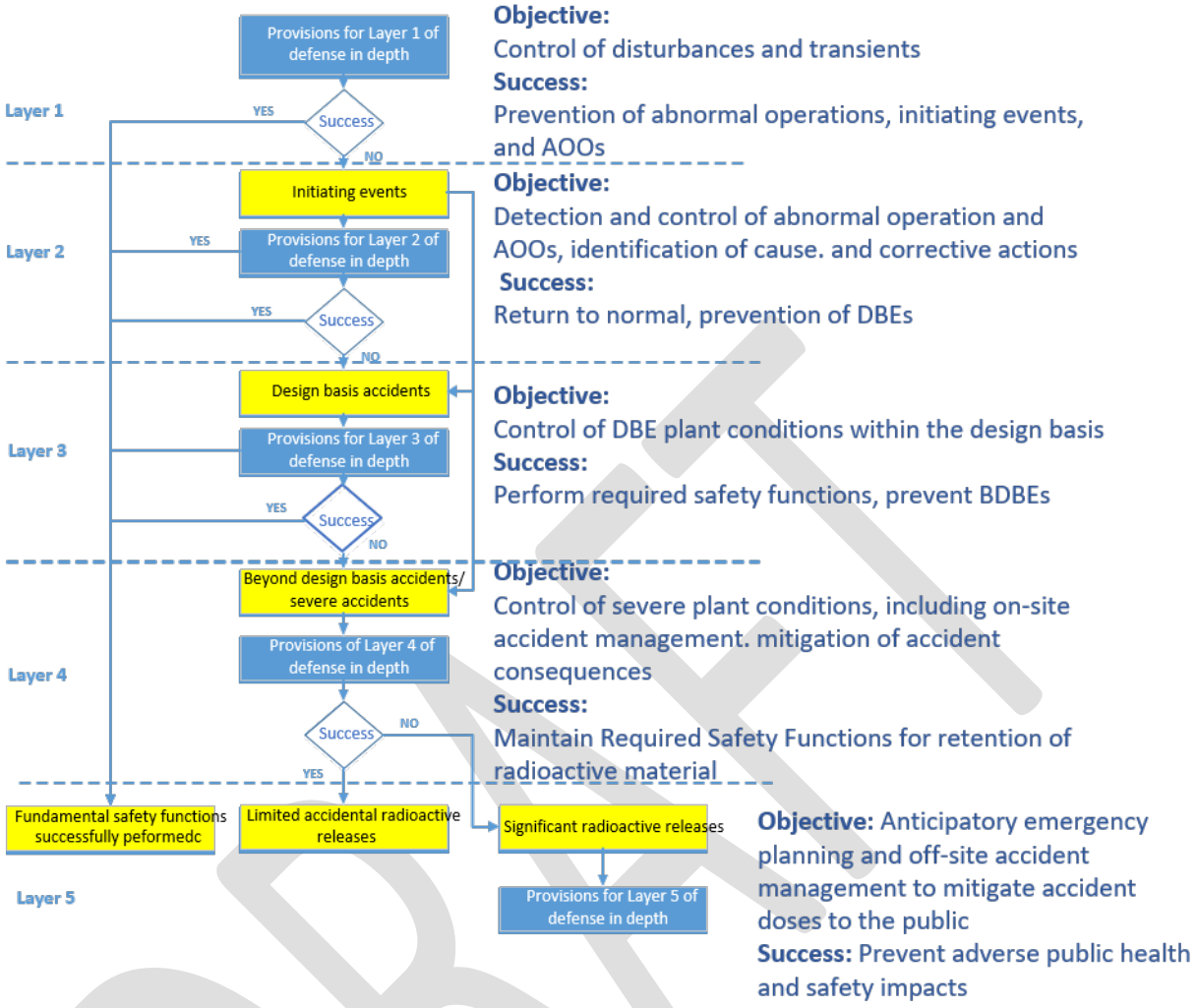

Figure 5-2. Framework for Evaluating LBEs Using Layers of Defense Concept Adapted from IAEA

A key element of the risk-informed, performance-based evaluation of DID is a systematic review of the LBEs against the layers of defense. LBE evaluations 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?

In this methodology, an IDP, is utilized for evaluating the adequacy of DID. How the process is implemented may vary depending on the state of design development, construction or operations. Adequacy of DID is confirmed when the following actions and decisions by the IDP are completed.

Plant capability DID is deemed to be adequate when:

- Plant capability DID guidelines in Table 5-1 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 when:

- 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.

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.

6 REFERENCES

(To be provided in the future)

7 GLOSSARY OF TERMS

Table 7-1. Glossary of Terms

Term	Acronym	Definition
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.
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 typically classified as BDBEs (may vary for each country). BDBEs take into account the expected response of all SSCs within the plant regardless of safety classification.
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. DID includes the use of access controls, physical barriers, redundant and diverse key SFs, and emergency response measures."
Design Basis Accident	DBA	Postulated accidents that are used to set design criteria and performance objectives for the design of SR SSCs. DBAs are derived from DBEs based on the capabilities and reliabilities of SR 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 applicable dose limits.
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 typically classified as DBEs (may vary for each country). 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.
Event Sequence	ES	A representation of a scenario in terms of an IEs defined for a set of initial plant conditions (characterized by a specified plant operating state [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 SFs along the event sequence.

Term	Acronym	Definition
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 DID.
Fundamental Safety Function	FSF	SFs common to all reactor technologies and designs; includes control heat generation, control heat removal and confinement of radioactive material.
Initiating Event	IE	A perturbation to the plant during a POS that challenges plant control and safety systems whose failure could potentially lead to an undesirable end state and/or radioactive material release. An IEs 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 IEs. 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 IEs 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 IEs may be identified as originating from a specific cause as defined in terms such as “flood-induced transient” or “seismically-induced RCPB breach.”
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 DID.
Licensing Basis Event	LBE	The entire collection of event sequences considered in the design and licensing basis of the plant, which may include one or more reactor modules. LBEs include AOOs, DBEs, BDBEs, and DBAs.
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.
Non-Safety-Related with NST SSCs	NST SSCs	All SSCs within a plant that are neither SR SSCs nor Non-SR SSCs with Special Treatment SSCs.
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 DID adequacy.
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

Term	Acronym	Definition
		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.
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.
Required Functional Design Criteria	RFDC	Reactor design-specific functional criteria that are necessary and sufficient to meet the RSFs.
Required Safety Function	RSF	A 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.
Risk-Informed	RI	An approach to decision-making in which insights from probabilistic risk assessments are considered with other sources of insights.
Risk-Significant SSC	--	An SSC that meets defined risk significance criteria. In the risk-informed 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 cumulative risk targets. The cumulative risk targets include: (i) maintaining the frequency of exceeding dose limit (e.g. 100 mrem in the U.S.) to less than 1/plant-year; (ii) meeting the safety goal QHO for individual risk of early fatality; and (iii) meeting the safety goal QHO for individual risk of latent cancer fatality.
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 SFs.
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.
Safety-Significant SSC	--	An SSC that performs a function whose performance is necessary to achieve adequate DID or is classified as Risk-Significant (see Risk-Significant SSC).