Southern Company

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

Fluoride-Cooled High Temperature Reactor
Licensing Modernization Project Demonstration

Authors: Matthew Denman, Jordan E. Hagaman, Grant Tinsley

Document Number
SC-29980-203 Rev 0

September 2019

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

Final issued by:

A Afzali

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

09/03/2019
Date

Disclaimer

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

Figures reflecting sequences, frequencies, consequences, or layers of defense are for illustration purposes only and do not reflect the final design or analysis of the KP-FHR.

Table of Contents

Disclaimer iii
List of Figures and Tables vi
List of Abbreviations vii
1.0 Introduction 1
1.1 Purpose 1
1.2 Scope 2
1.3 Objectives 2
1.4 Deliverables 2
1.5 Background and Linkage to LMP 3
1.5.1 LMP Guidance Document 3
1.5.2 LMP Documents 3
2.0 Demonstration Overview 5
2.1 Summary of Demonstration Activities 5
2.2 Prerequisites and Inputs for the Demonstration Project 5
2.2.1 PRA for Pre-Conceptual KP-FHR Design 5
3.0 LBE Selection 7
3.1 Brief Background on the PRA and Identified LBEs 9
3.1.1 Loss of Flow LOF-AOO-1 Event Sequence Family 12
3.1.2 Estimation of Consequences to the LBEs Identified by the PRA 14
3.1.3 KP-FHR LBEs Plotted Against the LMP Frequency-Consequence Target 15
3.2 Development of Required Safety Functions 16
4.0 Selection of Safety-Related SSCs 18
4.1 Identify Functions of Structures, Systems, and Components 19
Task 1. Identify SSC Functions in the Prevention and Mitigation of LBEs 19
Task 2. Identify and Evaluate SSC Capabilities and Programs to Support DID 21
Task 3. Determine the Required and Safety-Significant Functions 25
4.2 Evaluate Functions of Structures, Systems, and Components 28
Task 4a. Evaluate Functions Selected to Meet Required Safety Functions 28
Task 4b. Evaluate Non-Safety-Related SSC Functions for Risk-significance 29
Task 4c. Evaluate Non-Safety-Related SSC Functions Required for DID Adequacy 34
4.3 Classify Structures, Systems, and Components 36
Task 5a. Classify SSCs as Safety-Related 36
Task 5b. Classify SSCs as Non-Safety-Related with Special Treatment 38

4.4 Set Performance Targets for Structures, Systems, and Components 40
4.5 Determine SSC Specific Design Criteria and Special Treatment 40
Task 7a. Determine Required Functional Design Criteria, Safety-Related Design Criteria, and Special Treatment 41
Task 7b. Determine Non-Safety-Related SSC Special Treatment 43
4.6 Summary 44
5.0 Evaluation of Defense-in-Depth Adequacy 46
5.1 Evaluation of Risk-Informed and Performance-Based Defense-in-Depth 48
Task 1. Establish Initial Design Capabilities 48
Task 2. Establish Frequency-Consequence Target Based on Regulatory Objectives and Quantitative Health Objectives 49
Task 3. Define SSC Safety Functions for PRA Modeling 50
Task 4. Define Scope of Probabilistic Risk Assessment 52
Task 5. Perform Probabilistic Risk Assessment 53
Task 6. Identify and Categorize LBEs as AOOs, DBEs, or BDBEs 54
Task 7. Evaluate Licensing Basis Event Risks vs. Frequency-Consequence Target 55
Task 8. Evaluate Plant Risks Against Cumulative Risk Targets 55
5.2 Evaluation of Plant Capability Defense-in-Depth 57
Task 9. Identify Defense-in-Depth Layers Challenged by Each Licensing Basis Event 57
Task 10a. Select Safety-Related SSCs 58
Task 10b. Define Design Basis Accidents 60
Task 11. Perform Safety Analysis of Design Basis Accidents 61
Task 12. Confirm Plant Capability Defense-in-Depth Adequacy 62
5.3 Evaluation of Programmatic Defense-in-Depth 63
Task 13. Identify Non-Safety-Related with Special Treatment SSCs 63
Task 14. Define and Evaluate Required Functional Design Criteria for SR SSCs 65
Task 15. Evaluate Uncertainties and Margins 65
Task 16. Specify Special Treatment Requirements for SR and NSRST SSCs 66
Task 17. Confirm Programmatic Defense-in-Depth Adequacy 66
5.4 Summarize the Adequacy of Defense-in-Depth 67
Task 18. Defense-in-Depth Adequacy Established 67
6.0 Conclusions and Observations 68
6.1 Conclusions 68
6.2 Observations 69
7.0 References 71

List of Figures and Tables

Figure 1. Frequency-Consequence Evaluation Criteria Proposed for LMP from Reference [1] 7

Figure 2. Process for Selecting and Evaluating Licensing Basis Events from Reference [1]..... 8

Figure 3. Loss of Forced Flow Hierarchical Functional Systems Subsystem Initiating Event Relationship 10

Figure 4. Block Diagram for Loss of Flow Scenarios in Layers 2, 3, and 4 11

Figure 5. Loss of Forced Flow Event Tree..... 12

Figure 6. Loss of Flow (LOF-AOO-1) AOO versus Frequency-Consequence Target 15

Figure 7. Loss of Flow (LOF-DBE-1) DBE versus Frequency-Consequence Target 15

Figure 8. Loss of Flow (LOF-BDBE-1) BDBE versus Frequency-Consequence Target 16

Figure 9. Loss of Flow (LOF-BDBE-2) BDBE versus Frequency-Consequence Target 16

Figure 10. Definition of Required Safety Functions 17

Figure 11. Layers of Defense for the Loss of Flow Initiating Event Group 22

Figure 12. Example Determination of Risk-Significance Against Frequency-Consequence Curve 30

Figure 13. SSCs Performing Non-Safety-Related Reactor Control and Non-Safety-Related Decay Heat Removal Functions Control the Anticipated Loss of Flow and Prevent the Design Basis Loss of Flow 33

Figure 14. SSCs Performing Beyond Design Basis Reactor Control Functions Mitigate a Beyond Design Basis Loss of Flow to Within Quantitative Health Objectives 33

Figure 15. SSCs Performing Beyond Design Basis Decay Heat Removal Function Mitigate Beyond Design Basis Loss of Flow Events to Within Quantitative Health Objectives..... 34

Figure 16. Integrated Process for Incorporation and Evaluation of Defense-in-Depth 47

Figure 17. Frequency-Consequence Target Curve 50

Figure 18. Example of Prompt Health Risk of Licensing Basis Event Against a Target..... 56

Figure 19. Frequency of Exceeding 100 mrem at Site Boundary for Loss of Flow Events 57

Table 1. Adequacy of Plant Capability Defense-in-Depth 24

Table 2. Risk-Significance of Functions 31

Table 3. Safety-Significance of Functions..... 35

Table 4. Summary of Function Classifications 45

Table 5. Safety-Significance of Functions..... 64

List of Abbreviations

ANS	American Nuclear Society
AOO	Anticipated Operational Occurrence
ASME	American Society of Mechanical Engineers
BDBE	Beyond Design Basis Event
CFR	Code of Federal Regulations
DBA	Design Basis Accident
DBE	Design Basis Event
DID	defense-in-depth
DOE	Department of Energy
EAB	Exclusion Area Boundary
F-C	Frequency-Consequence
FHR	Fluoride-Cooled High Temperature Reactor
flibe	lithium fluoride-beryllium fluoride
KP-FHR	Fluoride-Cooled High Temperature Reactor
LMP	Licensing Modernization Project
non-LWR	non-light water reactor
NRC	Nuclear Regulatory Commission
NSRST	Non-Safety-Related with Special Treatment
NST	Non-Safety-Related with No Special Treatment
PRA	probabilistic risk assessment
QHO	Quantitative Health Objective
RIPB	risk-informed and performance-based
RVACS	Reactor Vessel Auxiliary Cooling System
SR	Safety-Related
SSC	structures, systems, and components
TRISO	tri-structural isotropic
U.S.	United States

1.0 INTRODUCTION

The Kairos Power Fluoride-Cooled High Temperature Reactor (KP-FHR) Demonstration Project described in this document directly supports the Licensing Modernization Project (LMP), a Southern Company-led, Department of Energy- (DOE) supported effort to achieve the desired technology-inclusive and risk-informed and performance-based (RIPB) pathway to licensing of advanced non-light water reactors (non-LWRs).

This report documents the evaluation of the KP-FHR Licensing Basis Events (LBEs) according to the process described in the LMP Guidance Document, NEI-18-04[1]. The scope of this demonstration addresses a limited scope table top application of the following aspects of the LMP methodology including the selection and evaluation of LBEs, safety classification of structures, systems, and components (SSCs), and evaluation of DID adequacy.

The approach taken here assumes that an initial selection of licensing basis events has already been made to match goals for the KP-FHR plant product, and uses the steps in NEI-18-04 to confirm the adequacy of those events for a safety case. The following text from the Guidance Document accommodates such an approach.

In some applications in which the Design Basis Accident (DBA) 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.

The Project's purpose, scope, objectives, and deliverables represent products supporting the LMP effort. These were developed in the project's initial charter and are summarized below.

1.1 Purpose

The purpose of the KP-FHR Demonstration Project was to exercise key LMP tasks as described in Guidance Document, NEI 18-04, in a limited scope manner that is sufficient to demonstrate the applicability of the LMP methodology to the KP-FHR. Each of the constituent components of the LMP methodology had been employed in previous DOE and industry initiatives with positive results; the Demonstration performed with Kairos Power was an opportunity to implement the process in the form described in the Guidance Document. Given the previous DOE and industry work which is foundational to the LMP, it was not the purpose of the KP-FHR Demonstration Project to determine whether the proposed process is feasible to implement or to justify the process by producing particular results—affirmative answers to those questions have long been observed and documented. The output of the Demonstration was used to inform the regulatory certainty of Kairos Power's FHR design and its associated safety design approach. Additionally, output of the Demonstration provided insights to the KP-FHR design-specific regulatory strategy. Insights from this project are expected to be useful to future users of the guidance in NEI 18-04.

1.2 Scope

The design used for this KP-FHR Demonstration was defined as Kairos Power's high temperature fluoride-cooled design and incorporating an initial probabilistic risk assessment (PRA) whose scope and level of detail are limited as appropriate for the pre-conceptual design status of the KP-FHR. This focused PRA was limited in scope and level of detail and includes only the Loss of Forced Flow Initiating Event (IE) with the plant operating at full-power. This limitation in scope and level of detail leads to a similarly focused demonstration of the LMP methodology.

The LMP process guidance used in this KP-FHR demonstration was the NEI 18-04 Guidance Document [1]. For this demonstration, the three main portions of the Guidance Document were demonstrated:

1. Selection of Licensing Basis Events (reference Section 3.0 of the Guidance Document)
2. Safety Classification and Performance Criteria for Structures, Systems, and Components (reference Section 4.0 of the Guidance Document)
3. Evaluation of Defense-in-Depth Adequacy (reference Section 5.0 of the Guidance Document)

1.3 Objectives

The objectives of the KP-FHR Demonstration were:

- Demonstrate key processes within the LMP Guidance Document applied to the KP-FHR. The application of the key processes was limited by the state of the KP-FHR design.
- Leverage the LMP process to inform the regulatory certainty of Kairos Power's FHR design and safety case, considering the current state of design, by identifying a credible spectrum of LBEs and investigating available SSC groupings that result in acceptable outcomes for the identified LBEs. Underlying this objective is the assertion that use of risk-informed, performance-based methods to reach these conclusions are endorsed by Commission policy and compatible with the existing regulatory framework.

1.4 Deliverables

The products of the Demonstration described in this document include inputs from:

- Licensing Basis Event (LBE) selection and evaluation, involving Anticipated Operational Occurrences (AOOs), Design Basis Events (DBEs), and Beyond Design Basis Events (BDBEs) and Identification of the Required Safety Functions [2]
- Safety Classification of SSCs [3]
- Assessment of Defense-in-Depth Adequacy [4]

1.5 Background and Linkage to LMP

The U.S. commercial nuclear power industry has long sought a broadly applicable, Nuclear Regulatory Commission- (NRC) accepted, RIPB licensing framework. Incremental advances, accelerated recently by increased interest in licensing advanced non-LWRs and Congressional interest, have resulted in an opportune time to pursue NRC endorsement of a RIPB framework. That framework is being advanced currently by the LMP, a Southern Company-led, DOE-supported effort to achieve the desired technology-inclusive, RIPB pathway to licensing of non-LWRs specifically. This Demonstration is an applied execution of the RIPB processes proposed by the LMP.

1.5.1 LMP Guidance Document

NEI is currently in the process of finalizing a stand-alone Guidance Document [1] describing the LMP processes for PRA development, selection, and evaluation of LBEs, SSC safety classification and performance requirements, and evaluation of defense-in-depth (DID) adequacy. The Guidance Document extracts important regulatory insights from a series of documents covering the same topics which describe the technical bases for the performance of RIPB decisions associated with designing and licensing advanced non-LWRs. The Guidance Document is intended to be endorsed by the NRC in the form of a Regulatory Guide for licensing advanced non-LWRs and is planned for release in 2019 [17].

1.5.2 LMP Documents

Probabilistic Risk Assessment Approach

The LMP PRA approach report contains the historical background, technical justifications and supporting information, and implementation guidance for creating a PRA model fit for providing insights into plant behavior for a given phase of design development for advanced non-LWRs. The LMP PRA approach is reactor technology inclusive and makes use of technology inclusive risk metrics. The PRA is recommended to be introduced at an early stage of design to incorporate risk insights into early design decisions. The PRA models are initially limited in scope and of a coarse level of detail as constrained by available supporting information. The scope and level of detail of the PRA models are increased as design and site information become available and as design features to protect the plant against internal and external hazards are defined. The RIPB decisions supported by the PRA and deterministic safety approaches are reviewed and revised as the risk model definition is brought into focus. The technical adequacy of the PRA for use in LMP applications is addressed by application of the ASME/ANS PRA Standard for Advanced non-LWRs, ASME/ANS RA-S-1.4-2013 [11], This LMP PRA Approach report is available as Reference [7].

Selection and Evaluation of Licensing Basis Events

Key to building the safety case of any reactor design is identifying, selecting, and evaluating Licensing Basis Events (LBEs), including the Design Basis Accidents (DBAs). The LMP proposed approach is designed to identify LBEs that reflect the reactor design and technology specific issues and challenges associated with each reactor's safety design approach. A systematic and prescriptive process is used to determine the safety functions required to meet risk targets, whose process provides the developer with options to select the safety-related SSCs

that will be used to demonstrate satisfaction of requirements for the Design Basis Accidents. This process builds on the PRA model and is tightly linked with the safety classification of SSCs. The report detailing this approach is available as Reference [8].

Safety Classification and Performance Criteria for Structures, Systems, and Components

Criteria are provided to classify SSCs into three safety classes: SSCs are either Safety-Related (SR), Non-Safety-Related with Special Treatment (NSRST) or Non-Safety-Related with no Special Treatment (NST). Based on the SSC safety functions in the performance of both prevention and mitigation functions, the developer assigns reliability and performance targets which help ensure that selected special treatment requirements are performance-based. This LMP SSC classification report is available as Reference [9].

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

The concept of DID has long been an expressed philosophy of commercial nuclear power design, licensing, and operation. An LMP report provides criteria for use by the reactor developer to systematically evaluate DID adequacy for the plant capabilities and programs that comprise DID, incorporate needed layers of defense to address uncertainties in the design and operation of the plant, and establish a fixed baseline of DID adequacy. This LMP report on DID is available as Reference [10].

2.0 DEMONSTRATION OVERVIEW

2.1 Summary of Demonstration Activities

The Demonstration progressed through the traditional project management phases: initiation, planning, execution, monitoring and controlling, and closeout. During the planning phase, a cross-functional, multi-company core team consisting of Southern Company, Kairos Power, and various industry experts was assembled. This team included subject matter experts on PRA, RIPB processes, technical project execution, and LWR fleet operations. Kairos Power personnel and their direct contractors performed the KP-FHR PRA analysis including consequence analyses, and provided design-specific engineering insights; Southern Company and industry consultants involved in the development of the LMP methodology provided project organization, guided the execution of the LMP RIPB process demonstration of the KP-FHR, and authored this report based on documents provided by Kairos that documented the results of each phase of the demonstration [2][3][4]. The LBE selection activities are summarized in Section 3.0. The Safety Classification of Structures, Systems, and Components activities are summarized in Section 4.0. The DID evaluation is summarized in Section 5.0. In Section 6.0 conclusions and observations from this Demonstration are provided.

2.2 Prerequisites and Inputs for the Demonstration Project

The focused PRA utilized for the KP-FHR Demonstration was developed during the pre-conceptual design phase. The PRA relied upon pre-conceptual design philosophies and engineering judgment for system reliabilities to provide a best-estimate of the expected event sequences and their associated frequencies. The purpose of the focused PRA was to demonstrate key elements of the LMP methodology and provide risk insights for the conceptual design development. As specified in the LMP PRA document, the goal of the PRA in the LMP approach is to support risk-informed decisions associated with each stage of design and licensing. The scope and level of detail of the PRA will be developed in stages and correspond to the scope and level of detail in each stage of design and licensing.

Given the current state of the design and available information, the focused PRA was limited in scope and level of detail to that of the pre-conceptual design and includes only the Loss of Forced Flow initiating event with the plant operating at full-power. As a result of this, the tasks to identify the design basis external events and to finalize the selection and evaluation of LBEs are deferred until greater design completion is achieved. However, even in this early phase of the design, the PRA included event sequences, sequence frequencies, and consequences. This section provides a description of some of the major inputs to the PRA development and key aspects of the PRA that are critical to the KP-FHR Demonstration.

2.2.1 PRA for Pre-Conceptual KP-FHR Design

The current scope of the PRA is characterized by the following:

- The at-power plant operating state is the initial focus of the risk assessment. This includes all plant challenges possible during power-delivery. Other operating state modes will be incorporated in the future as operational design information matures.

- Internal events, including mechanical, human, fire, and flood hazards are within the scope of the risk assessment. These hazards are studied at the plant-level and rely on screening based on anticipated equipment separation requirements. External hazards such as external flood, seismic, and high winds will be incorporated as the site envelope characterization for the KP-FHR is developed.
- System reliability is modeled by incorporating design reliability targets for individual and common cause failures. To characterize the reliability targets for yet-designed plant features, probability distributions expressing large uncertainties are used to ensure necessary visibility of passive and inherent design features are reflected in results in a manner that is consistent with the current state of knowledge about the safety characteristics of the KP-FHR.
- Success criteria, source term, and radiological consequences are defined in terms of retention requirements for radionuclide barriers. Similar to the system reliability figures, the uncertainty of yet-designed plant features is treated with probability distributions expressing large uncertainties to ensure that the final results adequately characterize the current state of knowledge for the design.

The PRA has the following outputs relevant to LBE selection and DID adequacy:

- Definition of LBEs in terms of event sequence families
- Frequency estimates with uncertainties for LBEs
- Consequence estimates with uncertainties for LBEs

3.0 LBE SELECTION

The LBE selection process follows the approach described in the LMP LBE selection and evaluation document [8] and Guidance Document [1]. The proposed Frequency-Consequence (F-C) Target used for the KP-FHR Demonstration and extracted from NEI 18-04 is shown in Figure 1. A design objective of the KP-FHR is to keep the LBEs well within the F-C Target such that the resulting margins can reflect the KP-FHR safety design approach and support the demonstration of DID adequacy.

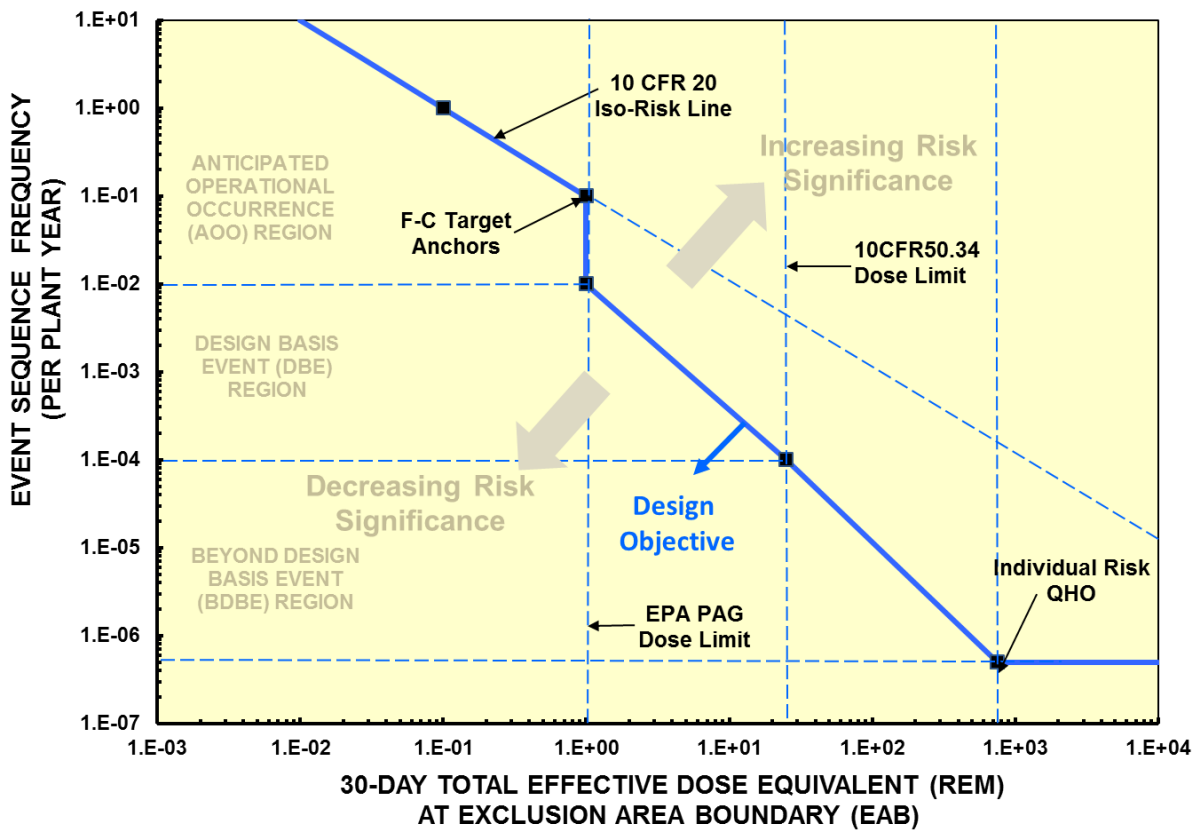

Figure 1. Frequency-Consequence Evaluation Criteria Proposed for LMP from Reference [1]

The LMP LBE selection and evaluation process is implemented as indicated in the steps on the flow chart shown in Figure 2 taken from NEI 18-04.* The LBE selection and evaluation steps of Figure 2 that were addressed in the Demonstration include Steps 3, 4, 5a, 5b, 6, and 7a-7e. Steps 1 and 2 had been performed for the pre-conceptual design prior to developing the PRA and prior to this demonstration. Steps 8, 9, and 10 are beyond the scope of this KP-FHR Demonstration.

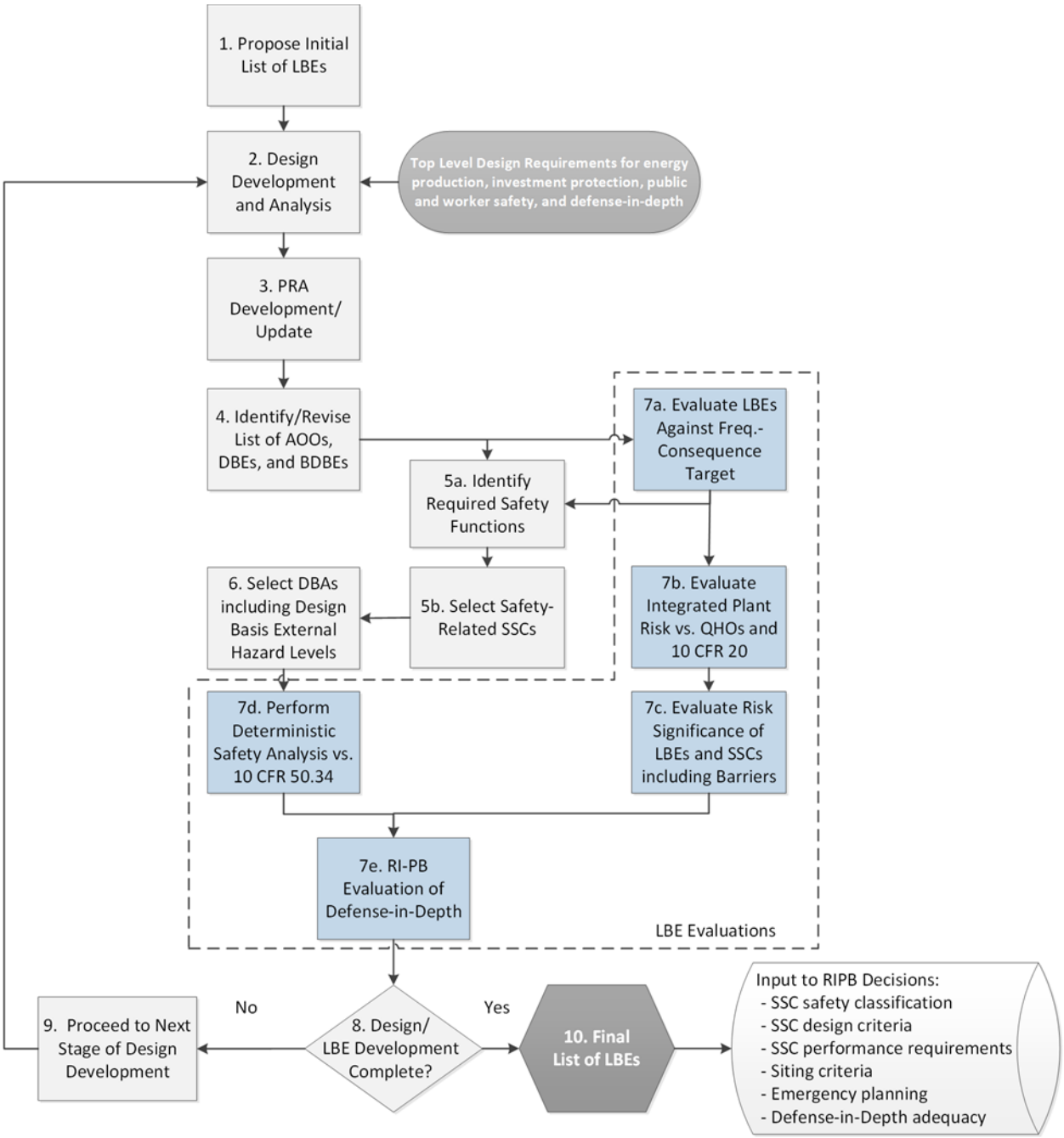

Figure 2. Process for Selecting and Evaluating Licensing Basis Events from Reference [1]

The LBE selection process begins with "Step 4. Identify/Revise List of AOOs, DBEs, and BDBEs." Then, "Step 7a. Evaluate LBEs Against Frequency-Consequence Target" is performed using the F-C Target shown in Figure 1. Information from this step is then used in Step 5a to identify the required safety functions and in Steps 5b to select the safety-related SSCs that are available to mitigate the spectrum of DBEs for each required safety function. This information can then be used to define the DBAs in Step 6 by deterministically assuming that the DBEs rely only on the safety-related SSCs.

However, before the LBEs in Step 4 can be defined, it was necessary to develop consequence estimates for each of the LBEs, as this information is not available from the preconceptual design KP-FHR PRA. Per the Advanced Non-LWR PRA Standard [11], these consequence estimates are to be developed using a mechanistic source term analysis and accompanying radiological consequence, dose, and dispersion analysis. It is the goal of the next version of the KP-FHR PRA to achieve this during the conceptual design phase. However, for the purposes of the KP-FHR Demonstration, consequences are developed using conservative estimates based on engineering judgement with large uncertainties assigned consistent with the current state of knowledge. This approach is comparable to that used in the Xe-100 Pebble Bed HTGR LMP Demonstration [16] which, like the KP-FHR PRA, had not progressed to the point where mechanistic source terms were available.

The tasks performed in the Demonstration to support Steps 4 and 7a of LBE selection process in Figure 2 include the following:

- Identify and categorize the risk-informed AOOs, DBEs, and BDBEs from the PRA by event sequence frequency
- Estimate the consequences for the LBEs
- Evaluate the LBEs against the F-C Target

3.1 Brief Background on the PRA and Identified LBEs

An important element of the PRA is the systematic search for IEs, which begins the process of event sequence modeling. The initial conditions for the selection of IEs for the KP-FHR PRA will eventually cover all operating and shutdown modes expected during the KP-FHR plant's operating life, including the expected shutdown configurations for conducting maintenance and inspections, and for the full range of internal and external events per the ASME non-LWR standard [11].

However, for the current scope and available design information, only the Loss of Forced Flow IE, at full power, is quantified using the PRA, for this demonstration. Consistent with the LMP PRA approach, consideration of external events and other modes other than full power is deferred to after the internal events at a future point in time when the design has progressed to such a level of detail that those analyses can be performed and produce actionable results for the designer.

To identify initiating events for the loss-of-flow event group, the hierarchical functional systems subsystem initiating event relationship [15, pp. 35–38] shown in Figure 3 was developed. Hierarchical functional system subsystem initiating event relationships provide a systematic approach for the identification of initiating events in compliance with the Standard's requirements [11]. These diagrams are a precursor to the development of master logic diagrams; both diagrams provide a top down functional description of the system while the master logic diagrams would extend this model to explicitly account for system redundancy and dependency.

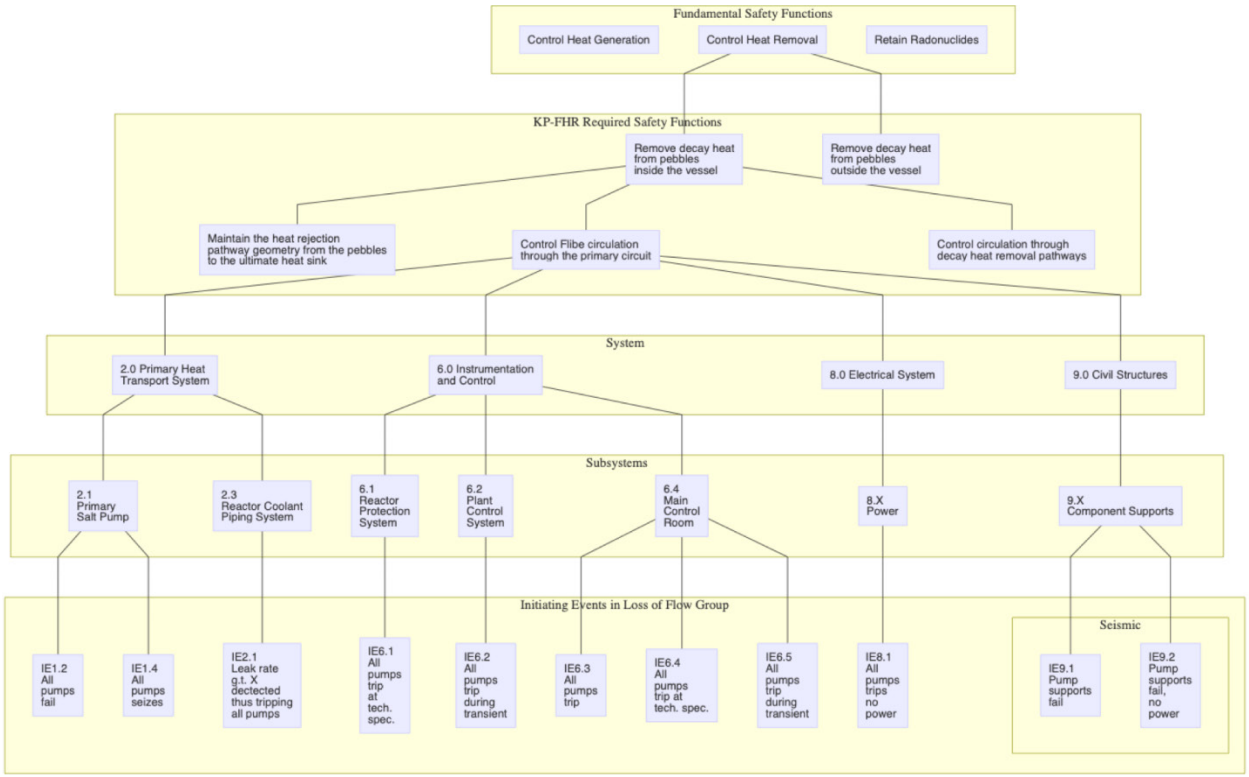

Figure 3. Loss of Forced Flow Hierarchical Functional Systems Subsystem Initiating Event Relationship

These relationship diagrams are developed via a top down approach where the Fundamental Safety Functions (FSFs) are listed at the top of the diagram. The KP-FHR derivative safety functions exist in the second layer of the diagram. The systems that are responsible for achieving a given safety function are enumerated in the third layer of the diagram. Subsystems that impact a given Systems ability to achieve a Safety Function are listed in the fourth row. If component level information is available, it would comprise the next layer of the diagram. Depending of the level of design fidelity available, initiating events that could impact the lowest system or component are enumerated for that subsystem or component. This approach allows for a systematic, structured, and traceable mapping of initiating events that could impact the facilities ability to achieve the desired safety function.

The types of initiating events that belong to this loss of forced flow initiating event group are summarized in the bottom row of Figure 3.

A simplified block diagram separating the levels of safety functions for the KP-FHR is shown in Figure 4. This diagram shows how non-safety-related, safety-related, and beyond design basis all work together to ensure adequate protection. As noted earlier, the LMP methodology is being used in this Demonstration to confirm earlier decisions that were made during the preconceptual design regarding design bases, the safety design approach, and SSC safety classification, rather than using LMP to derive these decisions along the way. This approach is recognized in NEI 18-04 as an acceptable means of implementing the LMP methodology. Non-safety and safety-related functions work together to ensure that the KP-FHR reaches a safe, stable shutdown while the beyond design basis functions, which may require operator actions, serve as a means of

mitigating releases from the site. Thus, both the reactor shutdown and decay heat removal systems have three layers of post-initiator functionality consistent with the LMP "layers of defense" concept:

- Layer 1 represents the design features responsible for preventing an initiating event.
- Layer 2 is the non-safety-related, normal system functional response to a loss of flow transient.
- Layer 3 is the safety-related functional response of the system.
- Layer 4 is the beyond design basis function of the system. Reactor Vessel Auxiliary Cooling System (RVACS) is always a combined Level 3 and 4 function.

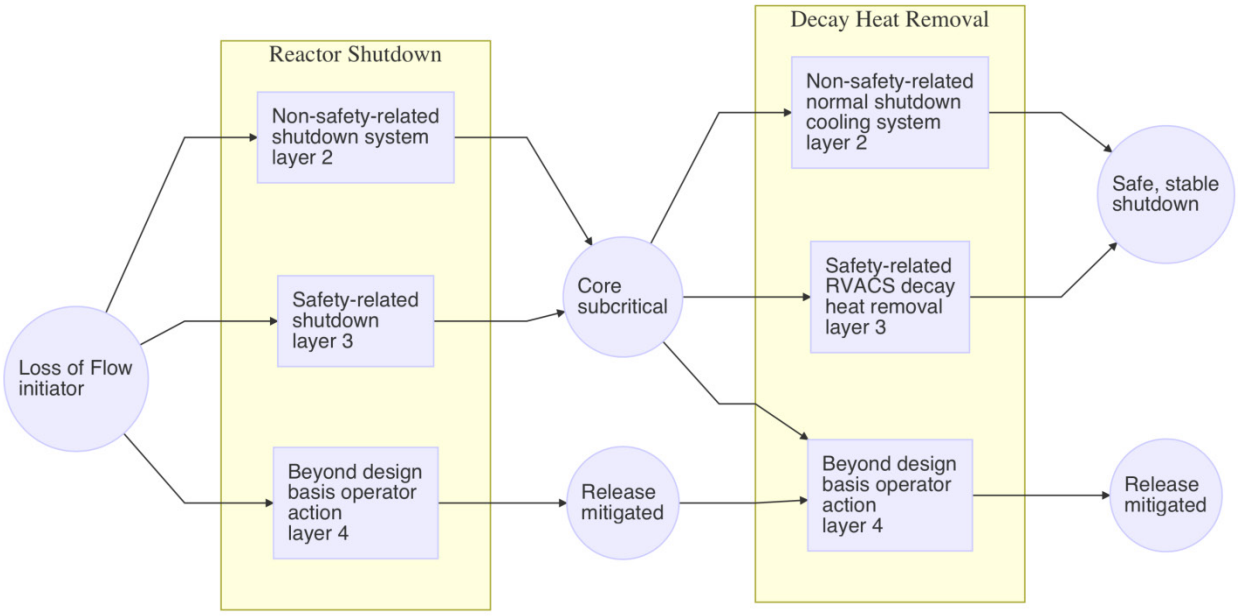

Figure 4. Block Diagram for Loss of Flow Scenarios in Layers 2, 3, and 4

The event sequences that result from the loss-of-flow initiating event group, with insights incorporated from the simplified block diagram, are displayed graphically in Figure 5, an event tree that describes the individual sequences considered in this analysis. The Loss of Forced Flow Event Tree, shown in Figure 5, illustrates a typical event tree from the PRA with the IE on the left (in units of per-plant-year, where a plant may be comprised of one or more reactor modules) and each of the branch points sequentially across the top for the plant response. For each branch point question, the Yes-No branches are shown with their estimated probability (no units). The final columns provide the overall event sequence frequency and the associated risk-informed LBEs in the three frequency ranges. The frequency basis is events per plant year, which is called for in evaluation of LBEs against the LMP F-C Target shown in Figure 1.

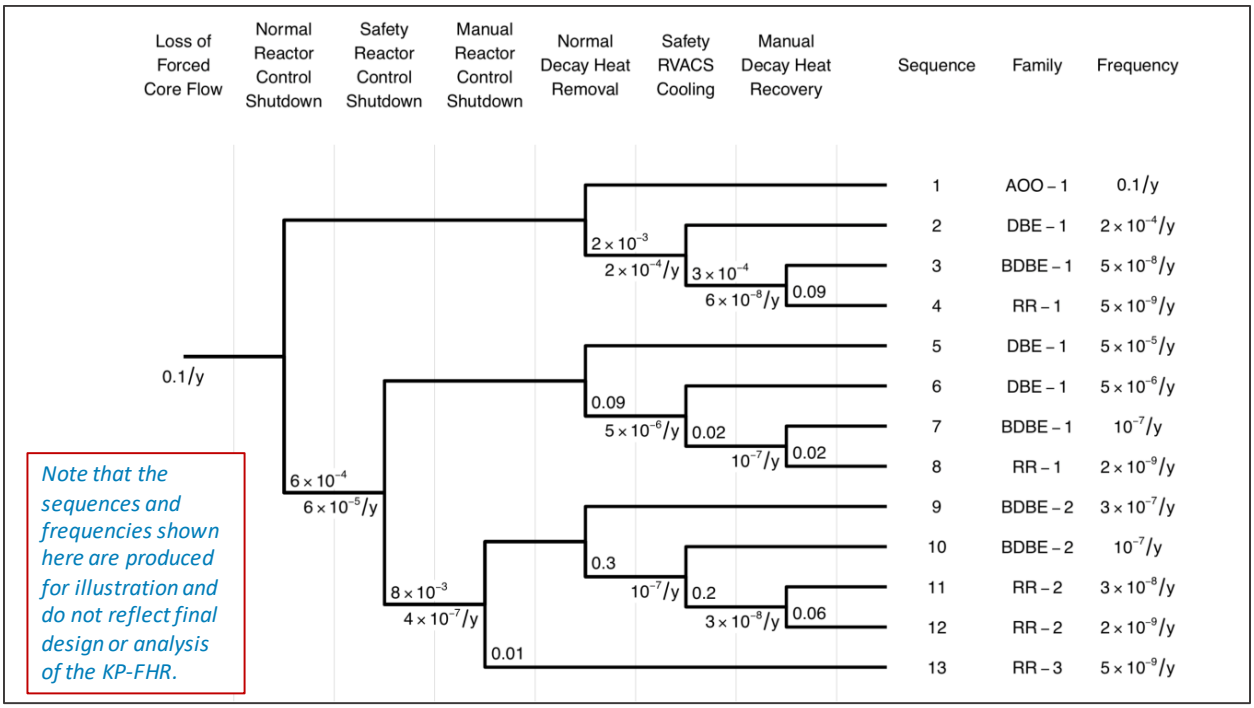

Figure 5. Loss of Forced Flow Event Tree

The modeling approach taken in the KP-FHR risk assessment is to use small event trees that reflect the simplicity of the plant response transients, supported by large fault trees that incorporate the reliability details and dependencies supporting the systems. Because of the dependencies, the conditional probabilities of failure for each system are highly dependent on the system successes and failures which precede it. This is due to functional dependencies among the systems that support the event tree top functions and the potential for intersystem common cause failures.

Using the parlance of the ASME/ANS Non-LWR PRA standard [11], event sequence families are defined in the risk assessment to group event sequences having similar plant response characteristics.

3.1.1 Loss of Flow LOF-AOO-1 Event Sequence Family

The event sequence family LOF-AOO-1 matches the anticipated loss of flow LBE described above. LOF-AOO-1 is a family containing a single event, Sequence 1, shown in Figure 5.

The loss of forced flow initiating event is a challenge to reactor temperatures, requiring an immediate reduction in core power and removal of residual decay heat. This is a demand on the normal reactor shutdown and decay heat removal systems. In this event sequence family, both the systems successfully operate and fulfill the fundamental safety functions for the plant.

3.1.1.1 Loss of Flow LOF-DBE-1 Event Sequence Family

The event sequence family LOF-DBE-1 matches the design basis loss of flow licensing basis event described above. LOF-DBE-1 is a family containing three events, Sequences 2, 5, and 6, shown in Figure 5.

Sequence 2 features a failure or unavailability of normal decay heat removal, with a demand on the safety decay heat removal through RVACS. Sequence 5 features a failure or unavailability of the normal reactor shutdown function, but a successful demand on the safety back-up that triggers insertion of the safety control rods. Sequence 6 is the same as sequence 5, but includes failure of both normal reactor shutdown and decay heat removal, and successful operation of both the safety shutdown and RVACS decay heat removal functions.

3.1.1.2 Loss of Flow LOF-BDBE-1 and LOF-BDBE-2 Event Sequence Families

The event sequence family LOF-BDBE-1 matches the anticipated loss of flow licensing basis event described above. LOF-BDBE-1 is a family containing two events, Sequences 3 and 7, shown in Figure 5.

Sequence 3 defines the beyond design basis conditions for a decay heat removal scenario. In this sequence, the normal decay heat removal system is failed or unavailable and the RVACS is degraded. Degraded RVACS conditions might be associated with an external event. In this sequence RVACS is not completely unavailable, but provides its function in such a way that design basis criteria on release are not met.

Sequence 7 is similar to sequence 3, but the starting conditions of the decay heat removal scenario feature the failure or unavailability of the normal reactor trip. This may result in additional core heat added to the system before the safety scram actuates and may be a more bounding challenge to structural temperatures. This sequence may involve operator actions to enhance RVACS heat removal capability or to realign normal decay heat removal.

The event sequence family LOF-BDBE-2 matches the anticipated loss of flow licensing basis event described above. LOF-BDBE-2 is a family containing two events, Sequences 9 and 10, shown in Figure 5.

Sequence 9 defines the beyond design basis conditions for a reactivity control scenario. In this sequence, the normal reactor shutdown system is failed or unavailable and the automatic safety control rods are also failed or delayed in inserting. This sequence relies on a combination of the performance of inherent reactivity feedback mechanisms of the core to reduce power on increasing temperature, as well as manual operator actions to recover the control rods.

Sequence 10 is similar to Sequence 9, but with the additional failure of normal decay heat removal. It is a challenge of operator actions to insert control rods and of RVACS to remove decay heat.

3.1.2 Estimation of Consequences to the LBEs Identified by the PRA

Currently, the consequences for LOF-AOO-1 are conservatively estimated. An upper-bound consequence of 2.5 mrem is assigned in lieu of detailed design calculations. This is conservative given that performance requirements for the non-safety-related functions are set such that effectively no release results from this event. If the performance requirement changes, this assessment will be updated to reflect that change. Further, as the design progresses, it will be evaluated against this consequence goal, with the effect of reducing uncertainty as the state of knowledge increases.

As noted in NEI-18-04, a 2.5 mrem 30-day dose at the exclusion area boundary is a reasonable *de minimis* dose [1, p. 25]. Therefore, no dose values less than this will be considered risk-significant. Further, doses that are shown at 2.5 mrem on the frequency-consequence chart should be considered less than or equal to 2.5 mrem, including those for LBEs that have effectively no release.

In this Demonstration, event sequence frequencies are derived from SSC reliability targets rather than derived in a "bottom up" fashion using PRA data. Consideration is given in the assignment of these targets to what is expected to be achievable for the current pre-conceptual design. In subsequent updates and upgrades of the PRA, the event sequence frequencies will be developed in a manner that meets the applicable data, human reliability analysis, and event sequence frequency quantification requirements in ASME/ANS RA-S-1.4-2013 [11].

The system performance targets for safety-related reactor shutdown and RVACS are defined such that for LOF-DBE-1, dose consequences can be calculated with high confidence to be less than 100 mrem.

Similar to the anticipated loss of flow, the consequences for LOF-DBE-1 are conservatively estimated. An upper-bound consequence of 100 mrem 30-day dose is set as a capability requirement for both safety-related functions. This model will be updated in the event that either (a) the capability requirement changes, or (b) detailed system design information becomes available to drive the inputs for a consequence analysis.

The operator actions and equipment design supporting both beyond design basis events, LOF-BDBE-1 and LOF-BDBE-2, are given performance targets with success criteria such that safety systems failed to maintain doses within 100 mrem, but successful plant contingencies are capable of maintaining consequences less than 1 rem.

As above, the consequences for LOF-BDBE-1 and LOF-BDBE-2 are both estimated through the application of the performance requirements shown on the frequency-consequence chart. This will be updated with detailed design calculations when design information is available. The effect of such updates will be a reduction in uncertainty to reflect an increased state of knowledge.

3.1.3 KP-FHR LBEs Plotted Against the LMP Frequency-Consequence Target

Figure 6 demonstrates that the anticipated loss of flow event (LOF-AOO-1) has acceptable risk based on the F-C Targets.

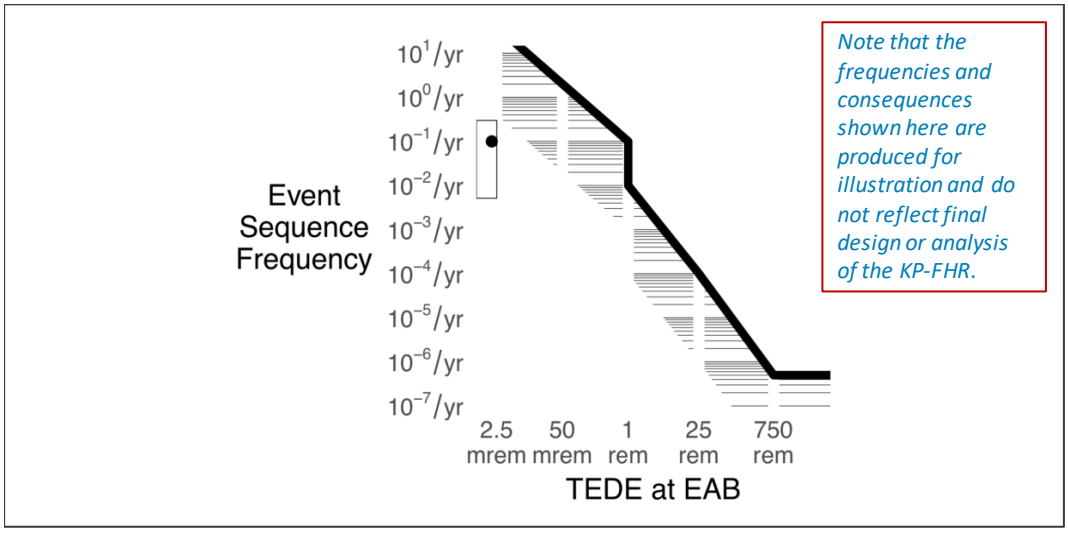

Figure 6. Loss of Flow (LOF-AOO-1) AOO versus Frequency-Consequence Target

Figure 7 demonstrates that the design basis loss of flow event (LOF-DBE-1) has acceptable risk based on the F-C Targets.

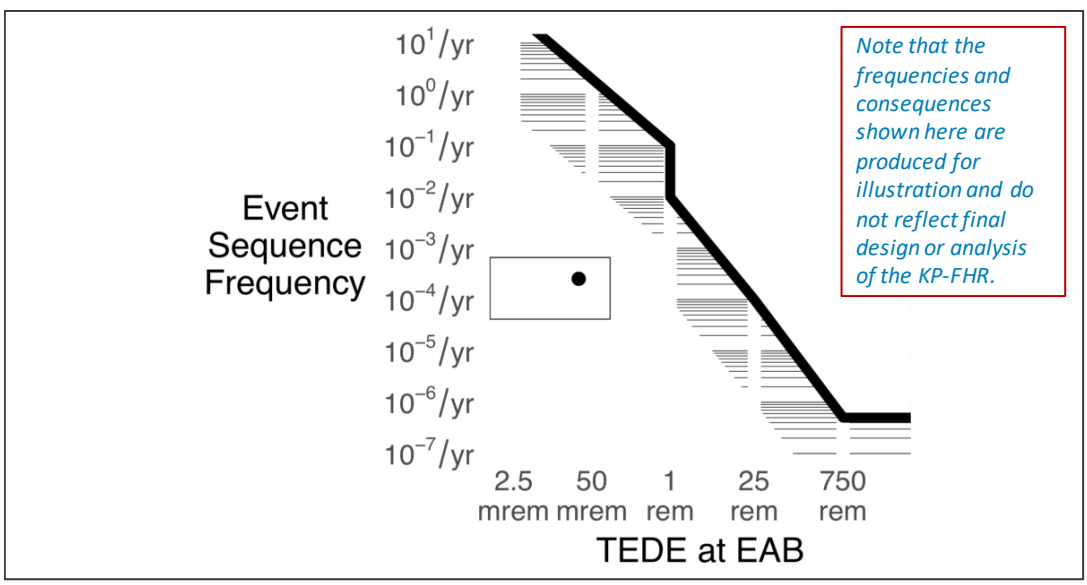

Figure 7. Loss of Flow (LOF-DBE-1) DBE versus Frequency-Consequence Target

The two beyond design basis events in this report (LOF-BDBE-1 and LOF-BDBE-2) have acceptable risk based on the F-C Targets, as shown in Figure 8 and Figure 9, respectively.

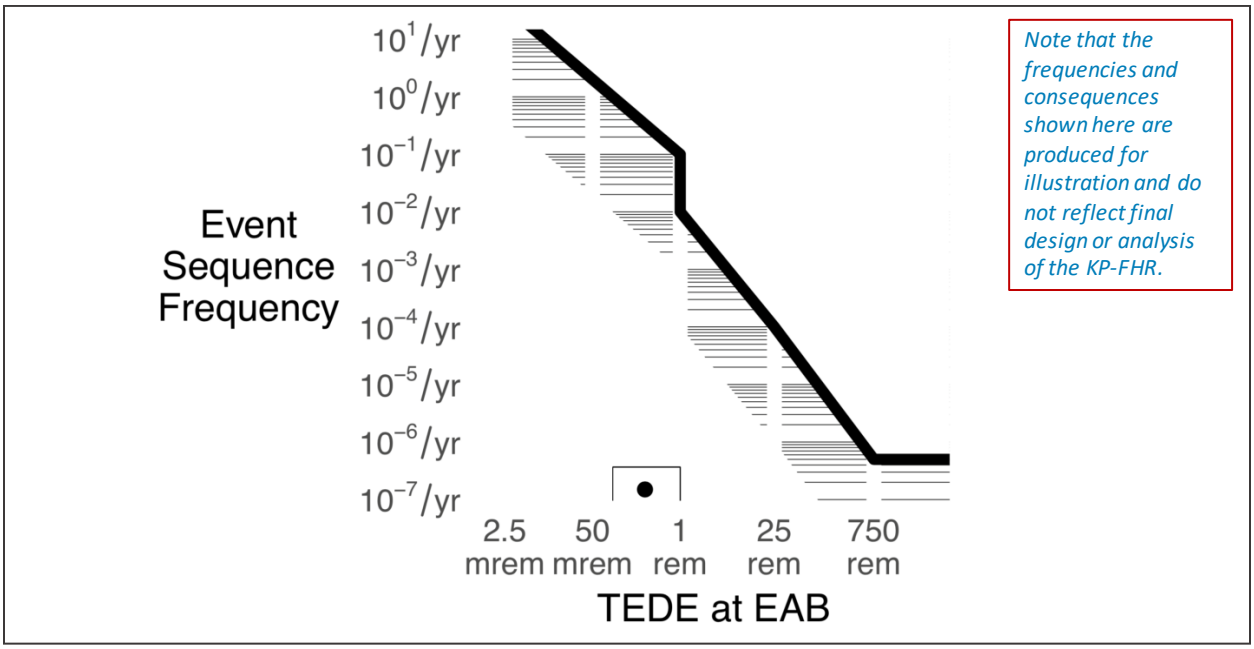

Figure 8. Loss of Flow (LOF-BDBE-1) BDBE versus Frequency-Consequence Target

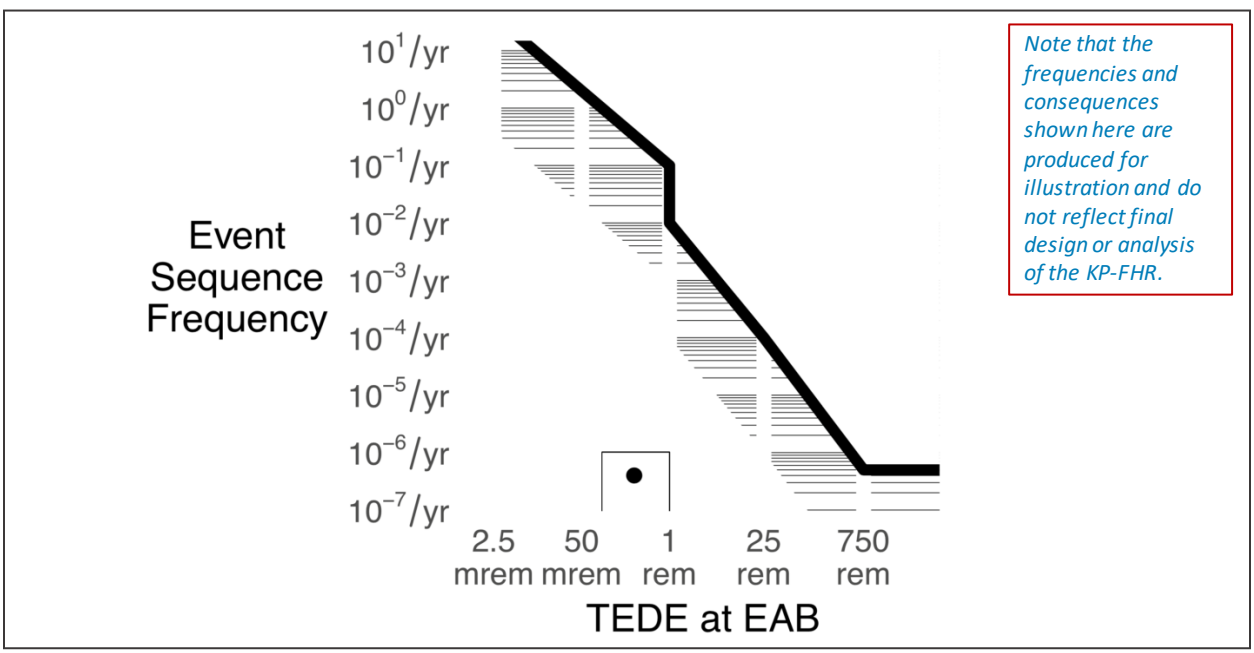

Figure 9. Loss of Flow (LOF-BDBE-2) BDBE versus Frequency-Consequence Target

3.2 Development of Required Safety Functions

The following functions are required to mitigate the design basis loss of flow, LOF-DBE-1:

- Safety reactor shutdown system initiates a reactor scram if a delay in the normal reactor shutdown occurs.

- Safety RVACS removes decay heat if the normal shutdown cooling system fails to do so.

Although not explicitly modeled in the event tree, two other required functions are performed:

- The reactor vessel is passively maintaining the geometry of the core coolant paths as well as retaining the primary flibe (lithium fluoride and beryllium fluoride) salt radionuclide barrier surrounding the fuel.
- The TRISO particles are all passively maintaining their radionuclide retention capability according to their qualification basis.

For all of the design basis events, the following high level Required Safety Functions are responsible for mitigating radiological consequences within 10 CFR 50.34 dose requirements. The Required Safety Functions are traced to the fundamental safety functions defined by the International Atomic Energy Agency for reactors. The fundamental safety functions are to control reactor power generation, control removal of power, and control the radionuclide material within the plant, as can be seen in Figure 10.

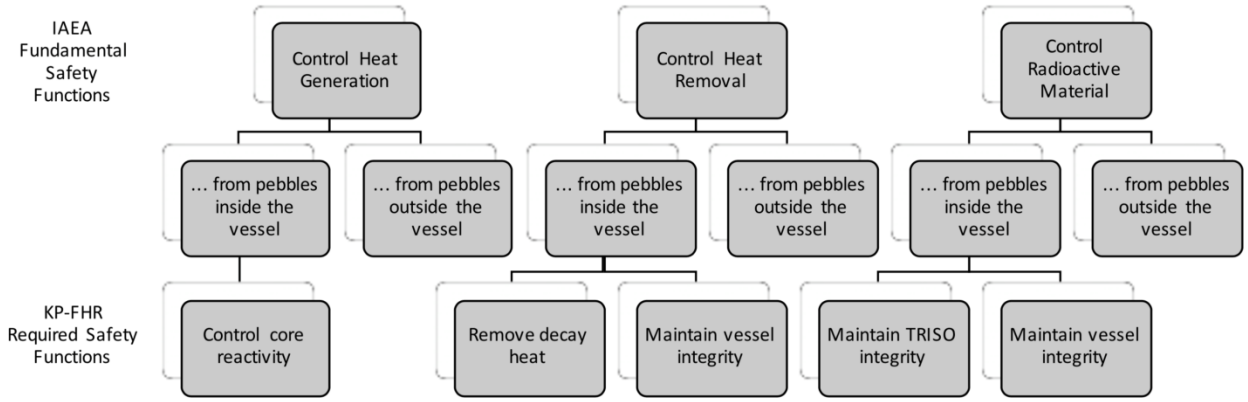

Figure 10. Definition of Required Safety Functions

Each of these functions is decomposed into reactor-specific functions for the KP-FHR. Heat generation is controlled by controlling the reactivity of the core. Heat removal is controlled using decay heat removal systems. Radionuclide material is controlled through a combination of the reactivity control and heat removal functions, as well as through the passive capability of the TRISO particles and reactor vessel to withstand the event conditions.

The required safety functions are decomposed into specific functions modeled in event sequences in the PRA.

4.0 SELECTION OF SAFETY-RELATED SSCS

This section documents the evaluation of the Kairos Power Fluoride-cooled High Temperature Reactor (KP-FHR) example equipment safety classifications according to the process described in the Licensing Modernization Project Guidance Document, NEI-18-04 [1]. The approach taken here:

- Assumes that the presented example safety classifications, including safety-related and non-safety-related with special treatment, are already selected as a matter of design objective to match goals for the KP-FHR plant product.
- Uses the steps in NEI-18-04 to confirm the example classifications for a safety case.

The following high-level tasks from the guidance document [1, pp. 30–35] are documented in this section for the validation of safety classification design decisions:

- Identify Functions of Structures, Systems, and Components
- Evaluate Functions of Structures, Systems, and Components
- Classify Structures, Systems, and Components
- Set Design Targets for Structures, Systems, and Components
- Determine Specific Design Criteria and Special Treatment

First, the functions that provide prevention and mitigation capability for licensing basis events are identified. The function capabilities of each structure, system, or component are determined to be a required safety function or a safety-significant function where necessary.

Second, each of the identified functions are evaluated. This includes the equipment functions that are selected to meet required safety functions in design basis accident conditions. This also includes an evaluation of risk-significance of each function against pre-determined criteria. The risk-significance criteria are defined against F-C Targets and targets associated with the integrated plant risk. Finally, functions are evaluated for their contribution to DID adequacy, even if they are not found to be risk-significant.

Third, each of the SSCs that are selected to perform the identified and evaluated functions are given classifications. These classifications include safety-related, non-safety-related with special treatment, and non-safety-related without special treatment.

Fourth, with each piece of plant equipment classified, performance targets are established for capability and reliability. These targets provide assurance that safety-related equipment is capable of performing required safety functions during design basis accidents. These targets also provide assurance that non-safety-related equipment is available to perform safety-significant functions.

Finally, special treatment requirements are defined. The purpose of any special treatment requirement is to provide adequate assurance that the SSC will perform the functions associated

with prevention and mitigation of licensing basis events. In accordance with the LMP methodology each special treatment is intended to assure that the SSC has adequate reliability and capability to perform these functions. The selection of specific special treatments is to be made as part of the Integrated Decision Process to assure adequacy of defense-in-depth.

4.1 Identify Functions of Structures, Systems, and Components

The functions that provide prevention and mitigation capability for licensing basis events are identified in this section. The function capabilities of each structure, system, or component are determined to be a required safety function or a safety-significant function where necessary.

The functions that form the safety case for the KP-FHR are identified in three tasks:

- Task 1. Identify SSC Functions in the Prevention and Mitigation of Licensing Basis Events
- Task 2. Identify and evaluate SSC capabilities and programs to support DID
- Task 3. Determine the Required and Safety-Significant Functions

The first task is to identify each of the licensing basis events and the prevention and mitigation functions that are relied upon in those events.

Next, the capabilities of plant equipment to support the DID case of the plant are identified. This includes formally introducing each function as a layer of defense for a licensing event.

Finally, these identified functions are characterized as a required safety function, a safety-significant function, or non-safety-significant function. Safety-significance of a function can be based on quantitative risk-significance evaluations or qualitative DID evaluations.

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

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

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

of this task is the identification of the SSC prevention and mitigation functions for all the licensing basis events.

4.1.1.1 Anticipated Operational Occurrences

All of the anticipated events must be demonstrated to not present conditions that would inhibit successful operation of the safety-related reactor shutdown system or the RVACS decay heat removal system. However, all of the anticipated events will also be demonstrated to avoid actuation of these systems to limit the demand frequency of safety-related systems. The Anticipated Loss of Flow event is presented below as an example.

Anticipated Loss of Flow (LOF.AOO.1)

A loss of power event which results in the loss of forced core flow and normal heat sink is an anticipated event. Responding to this event are automatic actuation of non-safety control system to detect the event and insert control rods to shut down the reactor. Additionally, this event is a challenge for the non-safety normal shutdown cooling system, which automatically actuates to remove decay heat.

The anticipated loss of flow can occur as a result of any the following:

- Loss of offsite power
- Loss of power due to switchyard failure
- Loss of power due to reactor building transformer failure
- Spurious primary salt pump trip
- Spurious cover gas depressurization

4.1.1.2 Design Basis Events

While any of the design basis events may result in successful actuation of non-safety reactor shutdown and non-safety normal shutdown cooling, the safety-related reactor shutdown system and RVACS decay heat removal are also available to perform their required safety functions. The design basis Loss of Flow event is presented below as an example.

Design Basis Loss of Flow (LOF-DBE-1)

A loss of power event concurrent with the unavailability of the normal reactor shutdown system or the normal shutdown cooling system is a design basis event. The unavailability of the non-safety systems results in an automatic actuation of the reactor shutdown system and RVACS decay heat removal system. This is a large group of events that include independent and common mode failures of systems concurrent with the initiator. For example, this event might include a design basis seismic event or an internal fire at the plant site.

In summary, the design basis loss of flow can include the following:

- Anticipated loss of flow with unavailability of non-safety-related reactor control

- Anticipated loss of flow with unavailability of non-safety-related normal shutdown cooling

4.1.1.3 Beyond Design Basis Events

Several beyond design basis events will be defined as design information matures. It is critical that these events be defined only after the design of safety-related equipment matures because these events represent the very rare conditions in which safety equipment is degraded such that it cannot perform the full required safety function.

The general characteristics of one type of beyond design basis event include failure of control and safety shutdown rods to shut down the reactor. These events rely on the inherent reactor feedback features of the core to naturally reduce core power to whatever heat removal capability is available. These events ultimately end in operator recovery of the failed control rod insertion and ultimate sub-criticality of the core.

The general characteristic of the second major type of beyond design basis event is a degradation of the performance of the RVACS decay heat removal system. Such degradation could include mechanical failure of actuation valves or passive conditions which limit the performance of RVACS. These events rely on the large heat capacity of the core and primary coolant to tolerate a delay in the actuation of decay heat removal. The events end in delayed operation of either the normal decay heat removal or RVACS.

The consequences of these events are shown to be within limits which might trigger offsite protection action guidelines.

Task 2. Identify and Evaluate SSC Capabilities and Programs to Support DID

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 licensing basis events, identification of the equipment responsible for the prevention and mitigation of accidents, and a set of criteria to evaluate the adequacy of DID. A result of this evaluation is the identification of functions, and the associated reliabilities and capabilities that are deemed to be necessary for DID adequacy. Such SSCs and their associated functions are regarded as safety-significant and this information is used to inform the SSC safety classification in subsequent tasks.

4.1.1.4 Layers of Defense

The design of plant response to various initiators is subdivided into a classical layers-of-defense paradigm, as shown in Figure 11.

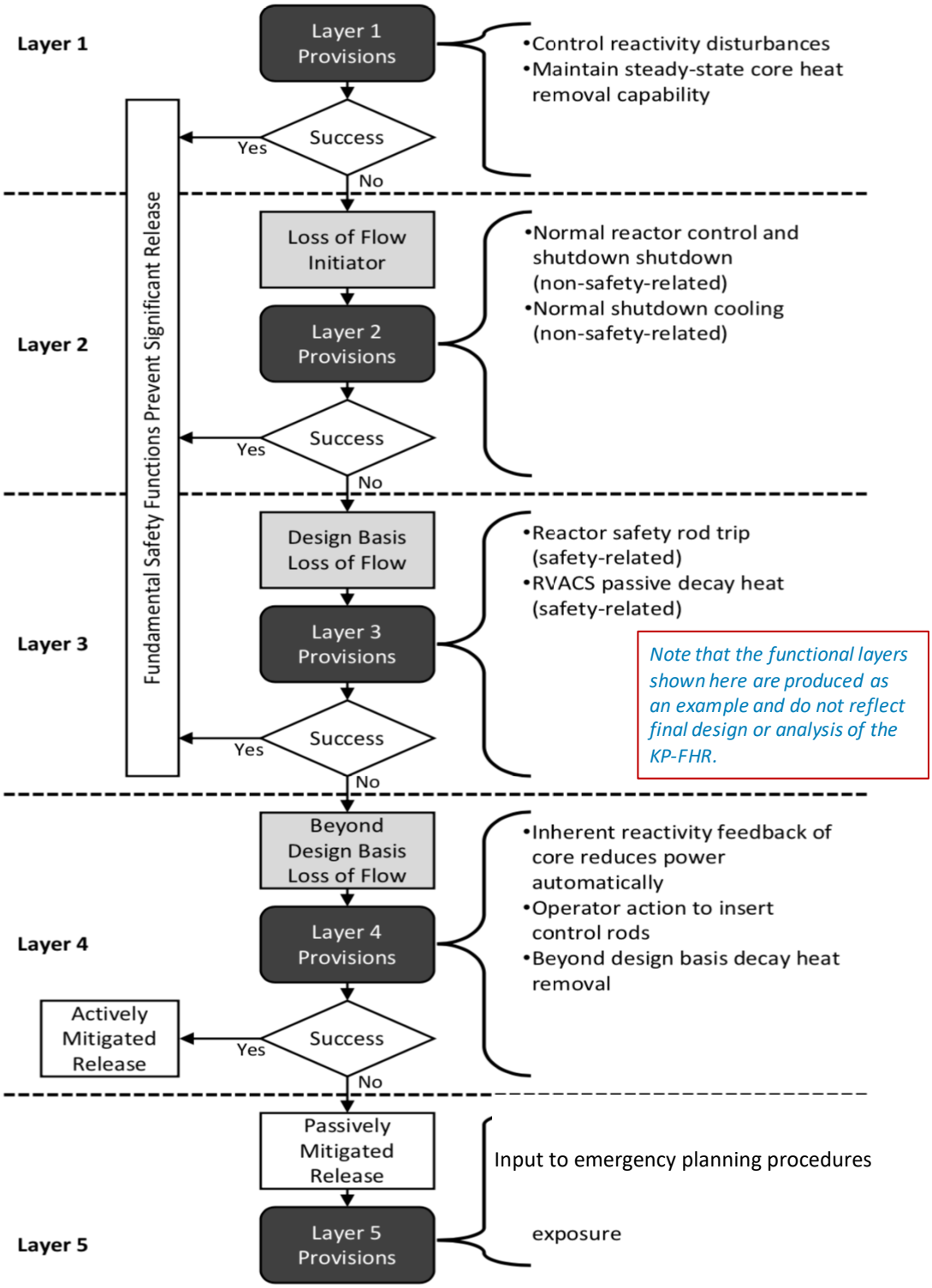

Figure 11. Layers of Defense for the Loss of Flow Initiating Event Group

The first layer of defense is represented by the plant's normal resilience to upset conditions through inherent and active control features. For a loss of flow event, the ability of the primary

core circulation pumps to maintain a flow rate in steady-state is the first line of defense against release.

The second layer of defense is represented by the plant's response to a failure of the first layer of defense. This presents the initiating event that is referred to in this work as the anticipated loss of flow. This event presents a challenge to the non-safety-related front-line systems that are responsible for guaranteeing that the plant can be placed in a safe and stable condition following the initiating event.

The third layer of defense is represented by the failures of Layer 1 (initiating loss of flow) and Layer 2 (unavailability of one of the front-line systems). This is a challenge to one or more safety-related systems. Either the safety control rods are demanded to make the reactor subcritical, or the safety-related RVACS system is actuated to remove decay heat. The end state of successful Layer 3 operation is a safe and stable condition.

The fourth layer of defense treats the rare case of concurrent failures of Layer 1 (initiator), Layer 2 (non-safety-related equipment), and Layer 3 (safety-related equipment). This is a beyond design basis event that is a challenge to systems and operator actions to recover failed functions under extreme conditions. The result of these events is not necessary a safe and stable condition, but is measured by the mitigation of radionuclide release.

The fifth and final layer of defense considers the failure of systems and operator actions to recover from failures of safety-related systems. These events may end in a release that is not actively mitigated, but is still passively mitigated by the inherent features of the plant. Such features include the low operating pressure which will limit the transmission of a source term, as well as the high-retention TRISO fuel and the radionuclide solvency of the primary coolant salt (flibe).

4.1.1.5 Plant Capability Defense-in-Depth

The plant capability DID is established by evaluating each layer of defense against qualitative and quantitative criteria. For each layer, quantitative objectives are focused on meeting F-C Targets and cumulative risk metrics with sufficient margin. The level of margin between the licensing basis event risk and health objectives provides evidence of plant capabilities for DID.

Additionally, qualitative objectives are in place to ensure that no single design or operational feature is relied upon to satisfy all layers. This criteria applies no matter how robust a particular structure, system, or component is established to be.

The following sections provide the evaluation of each identified PRA function against quantitative and qualitative DID adequacy criteria. This evaluation establishes evidence that the plant design and operational features and protective strategies employed to support each layer are functionally independent. Table 1 summarizes the key constraints on this evaluation.

Table 1. Adequacy of Plant Capability Defense-in-Depth

Layer	Quantitative	Qualitative
1) Prevent off-normal operation and anticipated events	Maintain frequency of plant transients within design cycles	Meet owner requirements for plant availability
2) Control anticipated events and prevent design basis events	Maintain frequency of design basis events below 10^{-2}/yr	Minimize frequency of challenges to safety-related equipment
3) Control design basis events and prevent beyond design basis events	Maintain frequency of beyond design basis events below 10^{-4}/yr	No single design or operational feature relied upon to meet quantitative objective for all design basis events
4) and 5) Control beyond design basis conditions and prevent adverse impact on public health and safety	Maintain plant risks below health targets with sufficient margins	No single barrier or plant feature relied upon to limit releases for beyond design basis events

Prevent Off-Normal Operation and Anticipated Events (Layer 1)

Layer 1 DID is assured by non-regulatory owner requirements for plant reliability and availability. Design targets for transient cycles should limit the frequency of initiating events and transients.

Control Abnormal Operation, Detect Failures, and Prevent DBEs (Layer 2)

Layer 2 DID is assured by the normal engineered response of the plant to events that are likely to happen in the plant lifetime. This layer of defense often overlaps with the design features that owners rely upon for investment protection. Two major functions are identified in Layer 2:

- Non-safety-related reactivity control
- Non-safety-related normal shutdown cooling

Control DBEs Within the Analyzed Conditions and Prevent BDBEs (Layer 3)

Layer 3 DID is assured by the safety response of the plant to events that are unlikely to happen in the plant lifetime, but may happen in a large fleet of plants. This layer of defense uses many (if not all) of the SR SCCs in the plant. Two major functions are identified in Layer 3:

- Safety-related reactivity control
- Safety-related RVACS decay heat removal

Control Beyond Design Basis Conditions and Prevent Adverse Impact on Public Health and Safety (Layer 4)

Layer 4 DID is assured by the beyond design basis equipment and strategies to mitigate the consequences of the unlikely failure of safety-related systems. Two major functions are identified in Layer 4:

- Beyond design basis recovery of reactivity control
- Beyond design basis recovery of decay heat removal capability

Prevent Adverse Impact on Public Health and Safety (Layer 5)

Layer 5 DID is assured by a combination of passive plant features that mitigate the consequences of a credible source term. These features include the robustness of the TRISO fuel particles and the inherent radionuclide retention properties of the flibe salt coolant. In addition, simple building design and access control strategies prevent unauthorized persons from being impacted by high radiation areas inside the owner-controlled area of the plant.

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
- Required Safety Functions
- Other safety functions regarded as safety-significant

Safety-significant SSCs include those that perform risk-significant functions and those that perform functions that are necessary to meet 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 licensing basis events derived from the risk assessment include all the relevant SSC prevention and mitigation functions.

4.1.1.6 Required Safety Functions

This step involves identifying the functions that are essential to achieving a safe and stable end state for each of the design basis events. For this example, the only licensing basis event is the design basis loss of flow.

The design basis loss of flow matches the LOF-DBE-1 event sequence family. (See Figure 2.2, in the probabilistic risk assessment.

The following are characteristics of the design basis loss of flow event:

- This event groups all potential power and flow steady-state operating conditions that are part of at-power operation.
- This event also groups all anticipated values of core burnup.
- All events grouped in the design basis loss of flow begin with a loss of forced core flow. All possible behaviors of flow coast down are grouped together, with the most bounding variant characterizing the entire event.
- The event also groups all variations of this event where different temperature or flow measurements would trigger either the non-safety-related or the safety-related reactor

protection system to insert rods to assure safe shutdown. The family of events is bounded by the event where the safety-related system is used.

- The event also groups all variations of this event where different measurements could trigger non-safety-related or safety-related decay heat removal systems. These events include all anticipated timings of such an actuation. The family of events is bounded by the event where the safety-related RVACS is used.
- All events in the design basis loss of flow licensing event result in a safe, stable state is reached when the reactor is subcritical and vessel temperatures have reached the threshold defined for safe shutdown.

The following functions provide capability in mitigating the design basis loss of flow, LOF-DBE-1:

- Safety reactor shutdown system initiates a reactor scram if a delay in the normal reactor shutdown occurs.
- Safety RVACS removes decay heat if the normal shutdown cooling system fails to do so.

Although not explicitly modeled in the event tree, two other critical functions are performed:

- The reactor vessel is passively maintaining the geometry of the core coolant paths as well as keeping the primary flibe salt radionuclide barrier surrounding the fuel.
- The TRISO particles are passively maintaining their radionuclide retention capability according to their qualification basis.

For all of the design basis events, the following high level Required Safety Functions are responsible for mitigating radiological consequences within 10 CFR 50.34 dose requirements. The Required Safety Functions are traced to the fundamental safety functions defined by the International Atomic Energy Agency for reactors.

The fundamental safety functions are to control reactor power generation, control removal of power, and control the radionuclide material within the plant, as can be seen in Figure 10.

Each of these functions is decomposed into reactor-specific functions for the KP-FHR. Heat generation is controlled by controlling the reactivity of the core. Heat removal is controlled using decay heat removal systems. Radionuclide material is controlled through a combination of the reactivity control and heat removal functions, as well as through the passive capability of the TRISO particles and reactor vessel to withstand the event conditions.

The required safety functions are decomposed into specific functions modeled in event sequences in the PRA.

4.1.1.7 Mitigation of AOOs and Prevention of DBEs

The following functions mitigate the consequences of the anticipated loss of flow and reduce the frequency of the design basis loss of flow:

- Normal reactor shutdown system detects the loss of flow and inserts non-safety control rods.
- Normal shutdown cooling system removes decay heat.

Both of these systems have capability targets to fulfill their mitigation function in response to the anticipated loss of flow. Both of these systems also have reliability targets such that events where the system is unavailable to perform its function, which would be a design basis loss of flow, are rarer than 10^{-2}/year.

4.1.1.8 Mitigation of DBEs and Prevention of BDBEs

The following functions mitigate the consequences of design basis loss of flow and, along with the non-safety functions listed above, reduce the frequency of beyond design basis loss of flow events:

- Safety reactor shutdown system initiates a reactor scram if a delay in the normal reactor shutdown occurs.
- Safety RVACS removes decay heat if the normal shutdown cooling system fails to maintain reactor temperatures within acceptable limits.

As above, both of these systems have capability targets to fulfill their mitigation function in response to the design basis loss of flow.

Both of these systems also have reliability targets such that events where the system is unavailable to perform its function, which would be a beyond design basis loss of flow, are rarer than 10^{-4}/year.

4.1.1.9 Mitigation of BDBEs and Prevention of Residual Risk Events

The following functions mitigate the consequences of beyond design basis loss of flow events and, along with the non-safety and safety-related functions above, reduce the frequency of residual risk events:

- Equipment used by operators to manually initiate a reactor trip, or equipment used to repair failures of non-safety-related control rods or safety-related shutdown blades
- Equipment used by operators to manually initiate decay heat removal which did not actuate automatically, or equipment used to repair failures of normal shutdown cooling or RVACS

Both of these sets of equipment have capability targets to fulfill their mitigation function under the conditions defined by the beyond design basis loss of flow event. The conditions of the beyond design basis loss of flow events will be defined by the failure modes of the safety-related SSCs, which will be analyzed when detailed design information is available.

Both of these systems also have reliability targets such that events where the equipment is unavailable to perform its function, which would be a residual risk event eliminated from the licensing basis, are rarer than 5×10^{-7}/year.

4.2 Evaluate Functions of Structures, Systems, and Components

After the identification of functions, each of the functions are evaluated. This includes the equipment functions that are selected to meet required safety functions in design basis accident conditions. This also includes an evaluation of risk-significance of each function against pre-determined criteria. The risk-significance criteria are defined against F-C Targets and targets associated with the integrated plant risk. Finally, functions are evaluated for their contribution to DID adequacy, even if they are not found to be risk-significant.

- Task 4a. Evaluate functions selected to meet required safety functions
- Task 4b. Evaluate non-safety-related SSC functions for risk-significance
- Task 4c. Evaluate non-safety-related SSC functions required for DID adequacy

Task 4a. Evaluate Functions Selected to Meet Required Safety Functions

For each of the required safety functions identified in Task 3, specific functions from the PRA are selected to fulfill those required safety functions in all design basis events.

For this demonstration, two required safety functions are highlighted:

- Core reactivity control is accomplished in all identified design basis events by the safety-related reactor control function.
- Decay heat removal is accomplished in all identified design basis events by the safety-related RVACS decay heat removal functions.

These specific functions meeting required safety functions are evaluated with the defined design basis accidents. (For this document, only one is available.)

4.2.1.1 DBA Definitions

The design basis loss of flow (LOF-DBA-1) matches with the LOF-DBE-1 event sequence family from the PRA. In the design basis event, either the non-safety-related reactivity control system or the non-safety-related decay heat removal is unavailable. For the design basis accident, both non-safety-related systems are unavailable.

The following are characteristics of the loss of flow design basis accident (LOF-DBA-1):

- The reactor is operating at the most bounding power and flow steady-state condition before the onset of the transient.
- The burnup of the core is at the most limiting condition (likely equilibrium) for maximizing decay heat generation.

- The flibe salt is at the most limiting condition (likely end of life) for maximizing radionuclide inventories contained by the flibe salt.
- The event begins with an abrupt loss of forced core flow.
- The safety-related reactor protection system detects the need to insert safety shutdown blades through temperature or flow measurements within enough time to give margin to TRISO fuel temperature limits and vessel structural temperature limits.
- The safety-related RVACS initiates according to the safety-related sensors and logic. This may include a delay timer depending on the final design of the RVACS. The timing and capacity of RVACS will give margin to TRISO fuel temperature limits and vessel structural temperature limits.
- A safe, stable state is reached when the reactor is subcritical and vessel temperatures have reached the threshold defined for safe shutdown.

4.2.1.2 DBA Evaluations

This task corresponds to the traditional deterministic safety analysis that is found in the transient 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. The deterministic safety analysis uses the following high level criteria[2] for design basis accident calculations:

- 10 CFR 50.34(a)(2)(ii)(D)(1) An individual located at any point on the boundary of the exclusion area for any 2 hour period following the onset of the postulated fission product release, would not receive a radiation dose in excess of 25 rem total effective dose equivalent (TEDE).
- 10 CFR 50.34(a)(2)(ii)(D)(2) An individual located at any point on the outer boundary of the low population zone, who is exposed to the radioactive cloud resulting from the postulated fission product release (during the entire period of its passage) would not receive a radiation dose in excess of 25 rem total effective dose equivalent (TEDE).

The description of the evaluation model and results of calculations are the subject of future work.

Task 4b. Evaluate Non-Safety-Related SSC Functions for Risk-significance

An SSC is classified as risk-significant if the risk-significance criteria are met for any SSC function included within the licensing basis events. There are two sources of risk criteria.

The frequency-consequence curve is a tool for determining the risk-significance of SSCs that are responsible for the capability and reliability of fulfilling reactor safety functions. 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-safety-related SSCs perform functions that may be necessary to keep

AOOs or high-consequence DBEs within the F-C Target; these non-safety-related SSCs are also regarded as risk-significant and are classified as NSRST.

The risk-significance of a function performed by a system, structure, or component is depicted graphically by plotting on the frequency-consequence chart the licensing basis event or events where a given system is successful. Next, an additional LBE is represented on the chart, this LBE being similar but where the system fails or is otherwise unavailable to perform its function.

To assess the risk-significance of the system, the hybrid point on the frequency-consequence chart is marked where the upper bound frequency of the event with system success is matched with the upper bound consequence of the event where the system is unavailable. If that point is beyond the F-C Target, then that system was significant in keeping the licensing basis event group within the target and is therefore risk-significant.

If the hybrid point connecting system success frequency to system failure consequence falls beneath the F-C Target, then that system is not risk-significant according to this criterion. There is, however, additional criteria in this document that could cause the system to be risk-significant even if the hybrid point falls below the F-C Target in this exercise based upon the cumulative risk of all LBEs. Figure 12 provides two examples to illustrate this concept:

- Failure of the system would lead a that system being categorized as risk-significant because the LBE hybrid point moves above the F-C Target.
- Failure of the system would not lead a that system being categorized as risk-significant because the LBE hybrid point stays below the F-C Target.

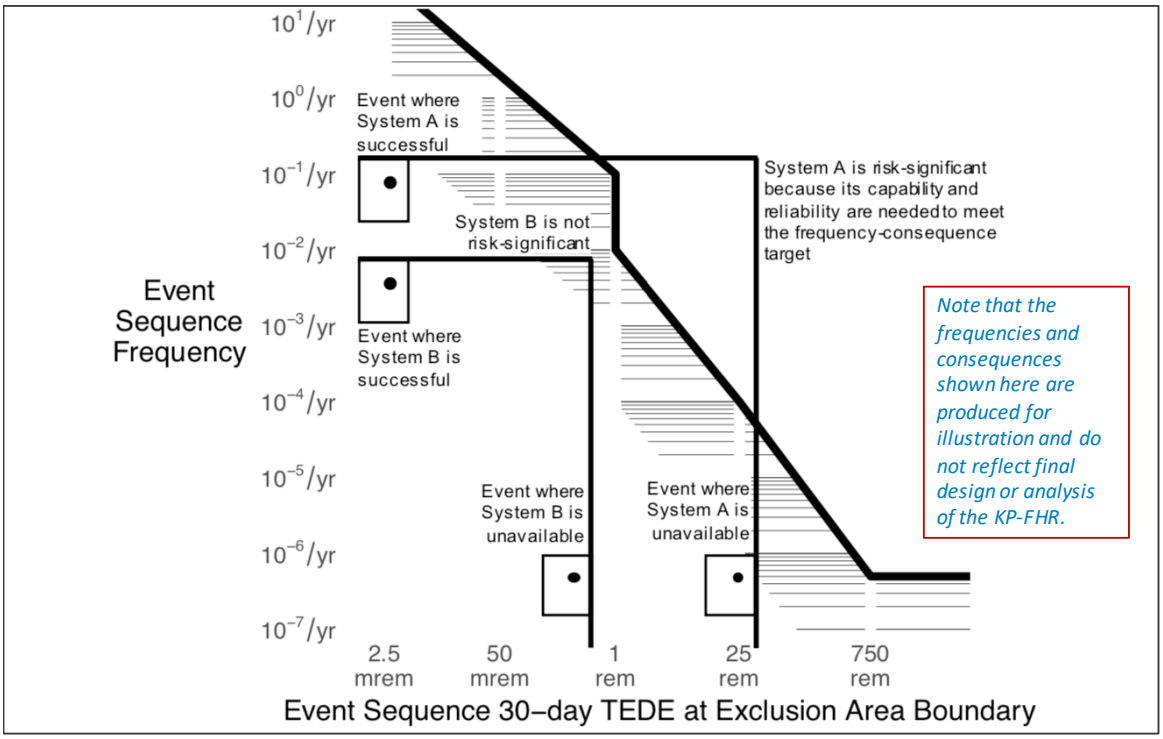

Figure 12. Example Determination of Risk-Significance Against Frequency-Consequence Curve

The second source of risk-significance criteria is in the cumulative risk metrics for the plant. 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 Exclusion Area Boundary (EAB) shall not exceed 5×10^{-7}/plant-year to ensure that the NRC Safety Goal Quantitative Health Objective (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.

Table 2 summarizes the findings from the risk-significance evaluation. Any function that is matches the risk criteria above is characterized as safety-significant.

Table 2. Risk-Significance of Functions

Function	Risk-Significant
Non-safety-related reactivity control	No
Beyond design basis reactor control	No
Non-safety-related decay heat removal	No
Beyond design basis decay heat removal	No

4.2.1.3 Risk-Significance of Non-Safety-Related Reactivity Control and Decay Heat Removal Systems

Non-safety-related reactivity control SSCs are not risk-significant based on the F-C Target. Additionally, non-safety-related normal shutdown cooling SSCs are not risk-significant based on the F-C Target.

The non-safety-related reactivity control equipment includes the following:

- Non-safety reactor control rods
- Control rod release and drive mechanisms
- Instrumentation to detect the need for reactor control (i.e. thermocouples, transducers)
- Logic equipment to translate instrument readings to shutdown signals
- Actuation equipment to release rods and/or drive rods into the core
- Support systems that ensure the availability of above
- Physical supports that secure the control rods and drives

The significance of reactivity control equipment can be measured by comparing the events where this equipment succeeds (anticipated loss of flow) and the events where this equipment fails (design basis loss of flow). The frequency of success and consequences of failure fall below the F-C Target.

The non-safety-related normal shutdown cooling equipment includes the following:

- Normal shutdown cooling piping, heat exchangers, and ultimate heat sink equipment
- Instrumentation to detect the need for decay heat removal (i.e. thermocouples)
- Logic equipment to translate instrument readings to actuation signals
- Actuation equipment to actuate normal shutdown cooling
- Structural supports for piping, heat exchangers, and ultimate heat sink equipment
- Support systems that ensure the availability of normal shutdown cooling to provide the decay heat removal function

Similar to Figure 12, Figure 13 shows how the significance of normal shutdown cooling equipment can also be measured by comparing the events where this equipment succeeds (anticipated loss of flow) and the events where this equipment fails (design basis loss of flow). The frequency of success and consequences of failure fall below the F-C Target.

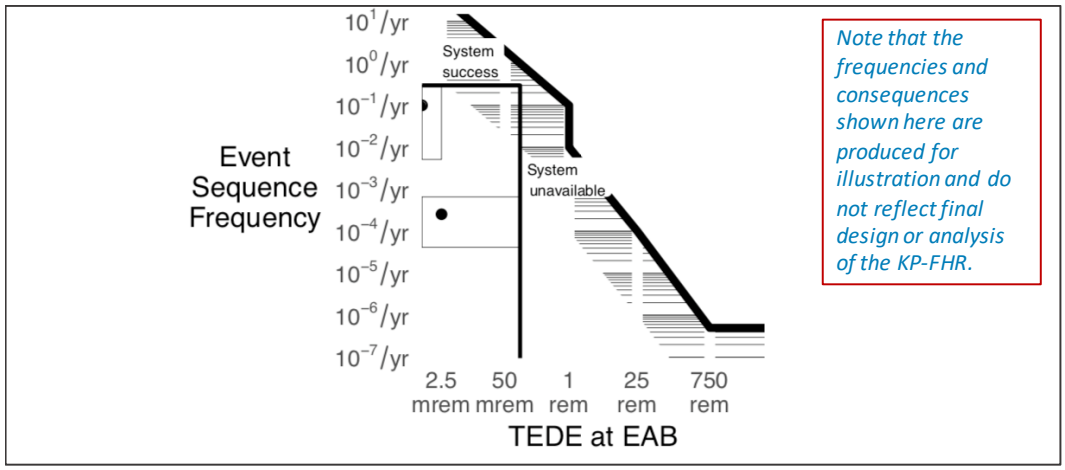

Figure 13. SSCs Performing Non-Safety-Related Reactor Control and Non-Safety-Related Decay Heat Removal Functions Control the Anticipated Loss of Flow and Prevent the Design Basis Loss of Flow

4.2.1.4 Risk-Significance of Beyond Design Basis Reactor Control

Beyond design basis reactor control SSCs are not risk-significant based on the F-C Target. The beyond design basis equipment for the reactivity control function includes:

- Control room or reactor building equipment used by operators to manually recover from a failure to scram automatically
- Structures that protect manways or operator access to critical control rod equipment to perform beyond design basis repair procedure actions
- Instrumentation and control systems that are critical to diagnosing failures

The significance of beyond design basis reactor control equipment can be measured by comparing the events where this equipment succeeds (LOF-BDBE-2) and the events where this equipment fails (RR-3). Figure 14 shows that the frequency of success and consequences of failure fall below the F-C Target.

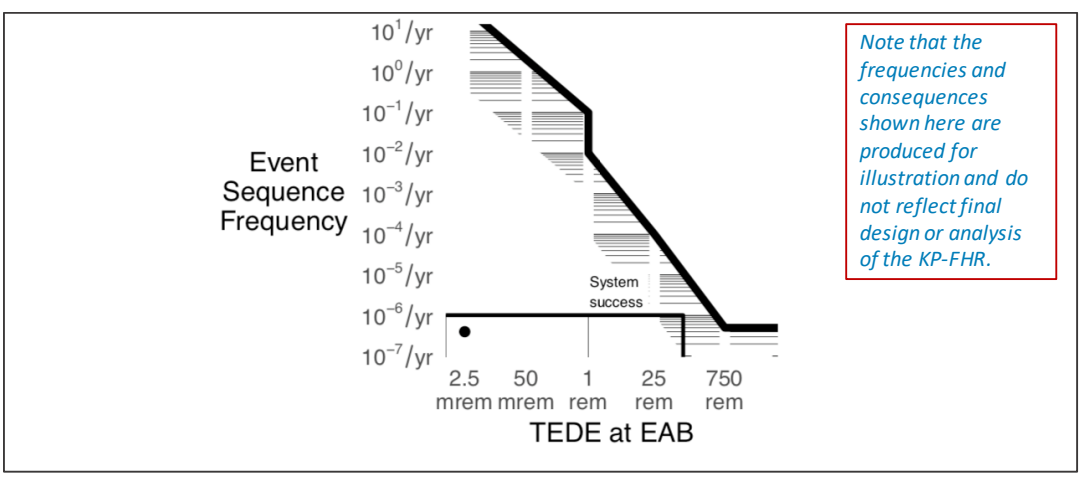

Figure 14. SSCs Performing Beyond Design Basis Reactor Control Functions Mitigate a Beyond Design Basis Loss of Flow to Within Quantitative Health Objectives

4.2.1.5 Risk-Significance of Beyond Design Basis Decay Heat Removal

Beyond design basis decay heat removal SSCs are not risk-significant based on the F-C Target.

The beyond design basis equipment for decay heat removal function include:

- Structures that protect manways or operator access to critical RVACS equipment to perform beyond design basis repair procedure actions
- Instrumentation and control systems that are critical to diagnosing failures

The significance of beyond design basis decay heat removal equipment can be measured by comparing the events where this equipment succeeds (LOF-BDBE-1) and the events where this equipment fails (LOF-RR-1). Figure 15 shows that the frequency of success and consequences of failure fall below the F-C Target.

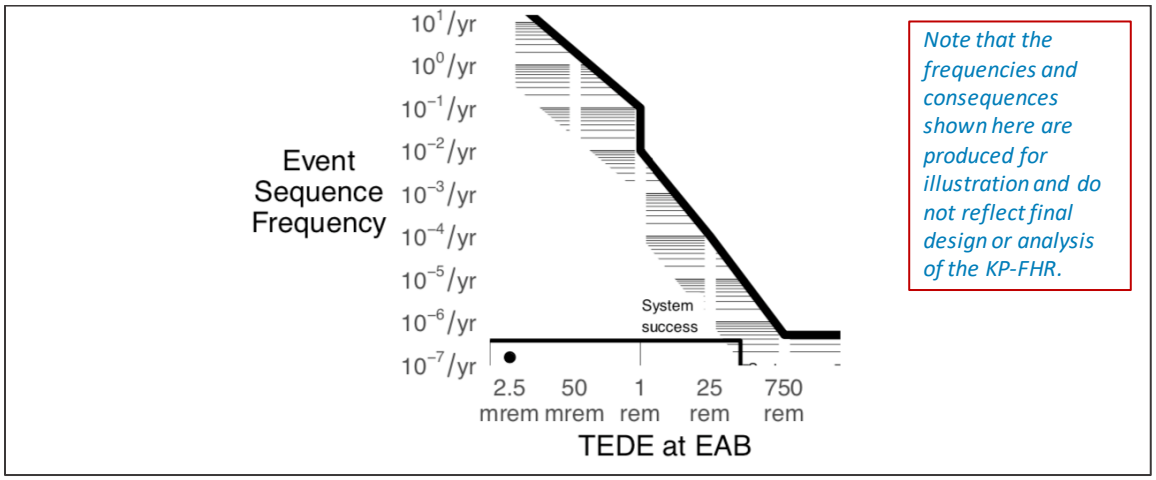

Figure 15. SSCs Performing Beyond Design Basis Decay Heat Removal Function Mitigate Beyond Design Basis Loss of Flow Events to Within Quantitative Health Objectives

Task 4c. Evaluate Non-Safety-Related SSC Functions Required for DID Adequacy

Any SSCs that do not meet the risk-significance criteria should be classified as safety-significant only if some form of special treatment is necessary to establish the adequacy of DID. The DID evaluation considers additional sources of uncertainty that are not fully resolved in the PRA, including measures to enforce assumptions made in the assessment, that may impact both frequencies and consequences and measures necessary to address considerations beyond the risk assessment. 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 safety-related or non-safety-related with special treatment. All non-safety-related without special treatment SSCs are not safety-significant. This provides a nexus between the SSC safety classification approach and the special treatment for safety-related and non-safety-related with special treatment SSCs.

Table 3 summarizes the findings from the significance evaluation for DID described in Task 2. Any function that is needed for DID is automatically characterized as safety-significant, regardless of the quantitative risk-significance determined by the PRA.

Table 3. Safety-Significance of Functions

Function	Risk-Significant	Needed for DID
Non-safety-related reactivity control	No	Yes
Beyond design basis reactor control	No	Yes
Non-safety-related decay heat removal	No	Yes
Beyond design basis decay heat removal	No	Yes

4.2.1.6 Control Abnormal Operation, Detect Failures, and Prevent DBEs (Layer 2)

Non-safety-related reactivity control SSCs are not risk-significant based on the F-C Target, but they do provide a DID function in reducing the frequency of DBEs below 10^{-2}/year. This equipment is therefore safety-significant, as shown below. Additionally, non-safety-related normal shutdown cooling SSCs are not risk-significant based on the F-C Target, but are safety-significant because of their function to reduce the frequency of DBEs.

Both of these functions and the SSCs performing the function are safety-significant because they simultaneously provide the following DID capabilities:

- Both functions control the anticipated loss of flow event.
- Both functions reduce the frequency of the design basis loss of flow event to below 10^{-2}/year.
- Both functions reduce the demand on safety-related systems.

4.2.1.7 Control Beyond Design Basis Conditions and Prevent Adverse Impact on Public Health and Safety (Layer 4)

Non-safety-related beyond design basis reactivity control SSCs are not risk-significant based on the F-C Target, but they do provide a DID function of ensuring that there is more than one contingency in response to the design basis loss of flow.

Both of these non-safety-related functions and the SSCs performing the functions provide the following DID capabilities:

- Both functions mitigate a beyond design basis loss of flow event.
- Both functions have capability and reliability that gives margins between licensing basis events and risk targets.
- Both functions will be designed to be recoverable in beyond design basis events, ensuring that no single design or operational feature is relied upon to meet risk criteria.

4.3 Classify Structures, Systems, and Components

Each of the SSCs that are selected to perform the identified and evaluated functions are given safety classifications. These classifications include Safety-Related, Non-Safety-Related with Special Treatment, and Non-Safety-Related with No Special Treatment.

- Task 5a. Classify SSCs as Safety-Related
- Task 5b. Classify SSCs as Non-Safety-Related with Special Treatment
- Task 5c. Classify SSCs as Non-Safety-Related with No Special Treatment

Task 5a. Classify SSCs as Safety-Related

This section defines the following safety functions for safety-related SSCs associated with mitigating loss of flow events:

- Control core reactivity
- Remove decay heat
- Maintain vessel integrity
- Maintain TRISO integrity

4.3.1.1 Control core reactivity

The following safety-related SSCs are designed to be available to automatically shut down the reactor following any of the design basis events:

- Reactor shutdown rods
- Shutdown rod release and drive mechanisms
- Instrumentation to detect the need for reactor shutdown (i.e. thermocouples, transducers)
- Logic equipment to translate instrument readings to shutdown signals
- Actuation equipment to release rods and/or drive rods into the core
- Support systems that ensure the availability of above
- Physical supports that secure the shutdown rods and drives
- TRISO particles and fuel, which provide a negative temperature coefficient of reactivity
- Vessel and graphite structures which maintain core geometry

The success of this fundamental safety function is measured by the subcriticality of the reactor and timing.

4.3.1.2 Remove Decay Heat

The following safety-related SSCs are designed to provide the fundamental safety function of removing core decay heat from the reactor following any of the design basis events:

- RVACS, including physical water storage tanks, cooling panels, valves, and associated equipment
- Instrumentation to detect the need for decay heat removal (i.e. thermocouples)
- Logic equipment to translate instrument readings to actuation signals
- Actuation equipment to open water valves and activate RVACS
- Structural supports for cooling panels
- Support systems that ensure the availability of RVACS to provide a passive decay heat removal function
- Air/water heat exchanger in RVACS stacks
- Physical RVACS chimneys
- Air intake structures
- Free-standing supports separate RVACS from the reactor building
- Any other equipment that can impact the passive and inherent features of the core that facilitate core heat removal

The success of this fundamental safety function is measured by salt temperature limits which are defined based on qualification temperatures of the TRISO fuel particles.

4.3.1.3 Maintain Vessel Integrity

The function to maintain vessel integrity also involves the use of the RVACS SSCs defined above. The function is defined separately because the success criteria to protect the vessel structure during accident conditions will have separate success criteria than the decay heat removal function. This function also serves to ensure that the primary salt coolant continues to surround the fuel pebbles for additional radionuclide retention.

In addition to the RVACS equipment identified above, vessel integrity also relies on the following:

- Reactor vessel
- Vessel supports stabilizing the vessel in the cavity
- Cavity seals preventing water ingress into the reactor cavity

The success of this fundamental safety function is measured by temperature limits, stress limits, and environmental qualification conditions set by the design life constraints of the reactor vessel.

4.3.1.4 Maintain TRISO Integrity

The consequences of all events with potential to release radionuclide material from the fuel are inherently limited by the assumed pre-transient conditions of the fuel. The fuel must therefore be monitored to provide high-confidence that the analysis conditions are not exceeded before the start of an accident.

The following safety-related SSCs are designed to ensure the pre-transient conditions of the TRISO fuel are within the analysis assumptions:

- TRISO fuel
- Instrumentation to detect the radionuclide inventory of the reactor cover gas space
- Instrumentation to detect the radionuclide inventory of the circulating salt coolant
- Instrumentation to detect unexpected transient failures from fuel pebbles circulating in the pebble handling system

The success of this fundamental safety function is measured by assurance that conditions exceeding the analysis assumptions for pre-transient damage to TRISO particles are maintained during normal operation.

Task 5b. Classify SSCs as Non-Safety-Related with Special Treatment

This section defines the equipment that provide defense layers for:

- Reactivity control
- Decay heat removal

4.3.1.5 Defense Layers for Reactivity Control

This section defines the reactivity control equipment that provides:

- Defense Layer 2
- Defense Layer 4

The equipment for Defense Layer 3 is omitted from this section, because it was already discussed as safety-related equipment above.

Defense Layer 2 Reactivity Control

The non-safety-related reactivity control equipment includes the following:

- Non-safety reactor control rods
- Control rod release and drive mechanisms
- Instrumentation to detect the need for reactor control (i.e. thermocouples, transducers)

- Logic equipment to translate instrument readings to shutdown signals
- Actuation equipment to release rods and/or drive rods into the core
- Support systems that ensure the availability of above
- Physical supports that secure the control rods and drives

Defense Layer 4 Reactivity Control

The beyond design basis equipment for the reactivity control function includes:

- Control room or reactor building equipment used by operators to manually recover from a failure to scram automatically
- Structures that protect manways or operator access to critical control rod equipment to perform beyond design basis repair procedure actions
- Instrumentation and control systems that are critical to diagnosing failures

4.3.1.6 Defense Layers for Decay Heat Removal

This section defines the decay heat removal equipment that provides:

- Defense Layer 2
- Defense Layer 4

The equipment for Defense Layer 3 is omitted from this section, because it was already discussed as safety-related equipment above.

Defense Layer 2 Decay Heat Removal

The non-safety-related normal shutdown cooling equipment includes the following:

- Normal shutdown cooling piping, heat exchangers, and ultimate heat sink equipment
- Instrumentation to detect the need for decay heat removal (i.e. thermocouples)
- Logic equipment to translate instrument readings to actuation signals
- Actuation equipment to actuate normal shutdown cooling
- Structural supports for piping, heat exchangers, and ultimate heat sink equipment
- Support systems that ensure the availability of normal shutdown cooling to provide the decay heat removal function

Defense Layer 4 Decay Heat Removal

The beyond design basis equipment for decay heat removal function include:

- Structures that protect manways or operator access to critical RVACS equipment to perform beyond design basis repair procedure actions

- Instrumentation and control systems that are critical to diagnosing failures

4.4 Set Performance Targets for Structures, Systems, and Components

Design targets for safety-related and non-safety-related with special treatment SSCs begin with the identification of the functions that are necessary to meet owner requirements for energy production, investment protection, worker and public safety, and licensing. 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 targets 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 structure, system, or component are sufficient for all the functions represented in the licensing basis events. A related priority is to provide reasonable confidence that the reliability and capability of the SSCs are achieved and maintained throughout the lifetime of the plant.

Those SSCs that are classified as safety-related are expected to meet applicable regulatory requirements as well as reactor-specific and design-specific safety-related design criteria derived from the required functional design criteria.

The following sections determine the target capabilities for each piece of safety-significant equipment:

- Task 6a. Determine safety-related SSC reliability and capability targets to perform required safety functions
- Task 6b. Determine non-safety-related SSC reliability and capability targets to perform safety-significant functions

Each of these tasks are out of scope given the level of current design detail and will be completed in future work.

4.5 Determine SSC Specific Design Criteria and Special Treatment

The purpose of special treatment is reflected in the Regulatory Guide 1.201 definition [3]:

> *"... 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 the NEI-18-04 process, this definition of special treatment is realized by those measures taken to provide reasonable confidence that plant equipment and features will perform their functions reflected in the licensing basis events. The applicable functions include those that are necessary to prevent initiating events and event sequences and other functions needed to mitigate the impacts of initiators on the performance of safety functions. Assurance is accomplished by achieving and monitoring the:

- Levels of reliabilities and availabilities that are assessed in the PRA and that are determined to be necessary to meet the licensing basis event risk evaluation criteria. These measures are focused on the prevention functions of the SSCs.
- Capabilities of the SSCs in the performance of their mitigation functions with adequate margins to address uncertainties.

The relationships between various reliabilities and capabilities in the performance of functions that are needed to prevent and mitigate event sequences are defined further in the next section.

The activities introduced above are a subset 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 here are evaluated as part of the DID adequacy evaluation. The actual set of special treatments applied to a given structure, system, or component are influenced by risk-informed performance-based considerations.

There are two tasks in this section:

- Task 7a. Determine Required Functional Design, Safety-Related Design Criteria, and special treatment
- Task 7b. Determine Non-Safety-Related SSC Special Treatment

Task 7a. Determine Required Functional Design Criteria, Safety-Related Design Criteria, and Special Treatment

As noted previously, SSCs classified as safety-related perform one or more safety functions that are required to perform either of the following:

- Mitigate design basis events within the F-C Target and design basis accidents within 10 CFR 50.34 dose limits
- Prevent any high-consequence beyond design basis events (those with doses exceeding 10 CFR 50.34 dose limits) from exceeding 10^{-4}/plant-year in frequency and thereby migrating into the design basis events region of the frequency-consequence evaluation

These required safety functions are used within this process to define a set of reactor-specific required functional design criteria. Safety-related design criteria are then derived from the functional design criteria. Because the required functional design criteria are 1) derived from a specific reactor technology and design, 2) supported by a design-specific PRA, and 3) related to a set of design specific required safety functions, the KP-FHR design process requires the development of a unique set of required functional design criteria. One purpose of the required functional design criteria is to form a bridge between the safety classification of SSCs and the derivation of SSC performance, special treatment requirements, and safety-related design criteria.

The process for identifying the required safety functions for a given reactor starts with a review of the safety functions modeled in the PRA for the prevention and mitigation of licensing basis events and identifying which of those safety functions, if not fulfilled, would likely increase the consequences of any of the design basis events beyond the F-C Target. This normally involves implementation of sensitivity analyses in which the performance of each safety function that mitigates the consequences of each design basis event is removed and consequences re-evaluated. From the required safety functions, a top-down logical development is used to define the functional requirements that must be fulfilled for the reactor design to meet each required safety function. The required functional design criteria 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 required safety function. The corresponding safety-related design criteria are then developed from the required functional design criteria.

While the requirements for the KP-FHR are still taking place, the following types of requirements will be added for non-safety-related equipment.

4.5.1.1 Requirements Associated with SSC Safety Classification

There are several core requirements for all equipment that gets a safety-related classification, including:

- Document basis for SSC categorization, which is verified by Integrated Decision-Making Panel
- Document evaluation of adequacy of special treatment to support SSC categorization, also verified by the Integrated Decision-Making Panel
- Change control process to monitor performance and manage SSC categorization changes
- Reliability Assurance Program including reliability and availability targets for SSCs in performance of PRA Safety Functions
- Design Requirements for SSC capability to mitigate challenges reflected in LBEs
- Maintenance Program that assures targets for SSC availability and effectiveness of maintenance to meet SSC reliability targets
- Licensee Event Reports
- 10 CFR 50 Appendix B Quality Assurance Program

This is the subject of future work once formal safety classifications are made on the detailed design.

4.5.1.2 4.5.1.2 Additional Special Treatment Requirements

The following list of special treatment will apply to each piece of safety-related equipment in the plant design:

- Required Functional Design Criteria

- Technical Specifications
- Seismic design basis
- Seismic qualification testing
- Protection against design basis external events
- Equipment qualification testing
- Materials surveillance testing
- Pre-service and risk-informed in-service inspections
- Pre-service and in-service testing

Task 7b. Determine Non-Safety-Related SSC Special Treatment

The safety classification of SSCs is made in the context of how the SSCs perform specific safety functions for each licensing basis event in which they appear. The reliability of the SSC serves to prevent the occurrence of the licensing basis event 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 licensing basis event.

The safety classification process and the corresponding special treatments serve to control the frequencies and consequences of the licensing basis events within the F-C Target and to ensure that the cumulative risk targets are not exceeded. The licensing basis event frequencies are a function of the frequencies of initiators 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 licensing basis event. 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 PRA Safety Function 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.

While the requirements for the KP-FHR are still taking place, the following types of requirements will be added for non-safety-related equipment with special treatment.

4.5.1.3 4.5.2.1 Requirements Associated with SSC Safety Classification

There are several core requirements for all equipment that gets a classification of non-safety-related with special treatment:

- Document basis for SSC categorization, verified by Integrated Decision-Making Panel

- Document evaluation of adequacy of special treatment to support SSC categorization, also verified by the Integrated Decision-Making Panel
- Document the evaluation of adequacy of special treatment to support SSC categorization
- Administration of a change control process to monitor performance and manage SSC categorization changes
- A Reliability Assurance Program including reliability and availability targets for SSCs in performance of PRA Safety Functions
- Setting Design Requirements for SSC capability to mitigate challenges reflected in LBEs
- A Maintenance Program that assures targets for SSC availability and effectiveness of maintenance to meet SSC reliability targets
- Creation of Licensee Event Reports
- A user provided Quality Assurance Program for non-safety SSCs

4.5.1.4 Optional Additional Special Treatment Requirements

The following list of special treatment might apply to each piece of non-safety-related with special treatment equipment in the plant design. The final decisions on adequacy of the special treatment will be verified by the Integrated Decision-Making Panel.

- Technical Specifications (event-specific)
- Seismic design basis (Seismic II/I requirements)
- Pre-service and risk-informed in-service inspections (event-specific)
- Pre-service and in-service testing (event-specific)

4.6 Summary

Section 4 above identified and evaluated the functions associated with a limited set of licensing basis events to demonstrate the method described in NEI-18-04 [1]. The functions were defined and evaluated in terms of risk-significance, significance to DID, and importance in fulfilling required safety functions for design basis accidents.

Table 4 presents a summary of each of the major functions described in this work as well as the result of the significance evaluations performed in this work. This table is represented in terms of functions to aid in the classification of SSCs once they are defined to fulfill those functions.

Table 4. Summary of Function Classifications

SSC Function	Risk-Significant	Safety-Significant	Safety-Related
Reactivity Control Functions			
Non-safety-related reactivity control	No	Yes	No
Safety-related reactivity control	No	Yes	Yes
SSCs separating non-safety from safety-related reactivity control	Yes	Yes	Yes
SSCs separating safety-related from beyond design basis reactivity control capability	Yes	Yes	Yes
Beyond design basis reactor control	No	Yes	No
Decay Heat Removal Functions			
Non-safety-related decay heat removal	No	Yes	No
Safety-related RVACS decay heat removal	No	Yes	Yes
SSCs separating non-safety from safety-related decay heat removal	Yes	Yes	Yes
SSCs separating safety-related from beyond design basis decay heat removal capability	Yes	Yes	Yes
Beyond design basis decay heat removal	No	Yes	No

5.0 EVALUATION OF DEFENSE-IN-DEPTH ADEQUACY

There are three primary focuses of this DID adequacy assessment:

- Risk-Informed and Performance-Based DID Adequacy
- Capability DID Adequacy
- Programmatic DID Adequacy

The RIPB DID adequacy focuses on developing and maintaining a basis for both supporting licensing basis event (LBE) selection as well as verifying that the entire plant conforms to cumulative risk targets.

The plant-capability DID adequacy assessment involves both the identification of the layers of defense and the definition of those SSCs which contribute to those layers of defense. The integration of deterministic design basis analysis is also a part of the plant capability DID adequacy.

Finally, the Programmatic DID adequacy assessment validates that appropriate treatment is given to the design, operation, and maintenance of safety-significant SSCs. This includes a definition of functional design criteria, an evaluation of uncertainties, and development of special treatment requirements to ensure that performance is maintained within the bounds of predictions.

The overall process for incorporation and evaluation of DID is illustrated in Figure 16 [1].

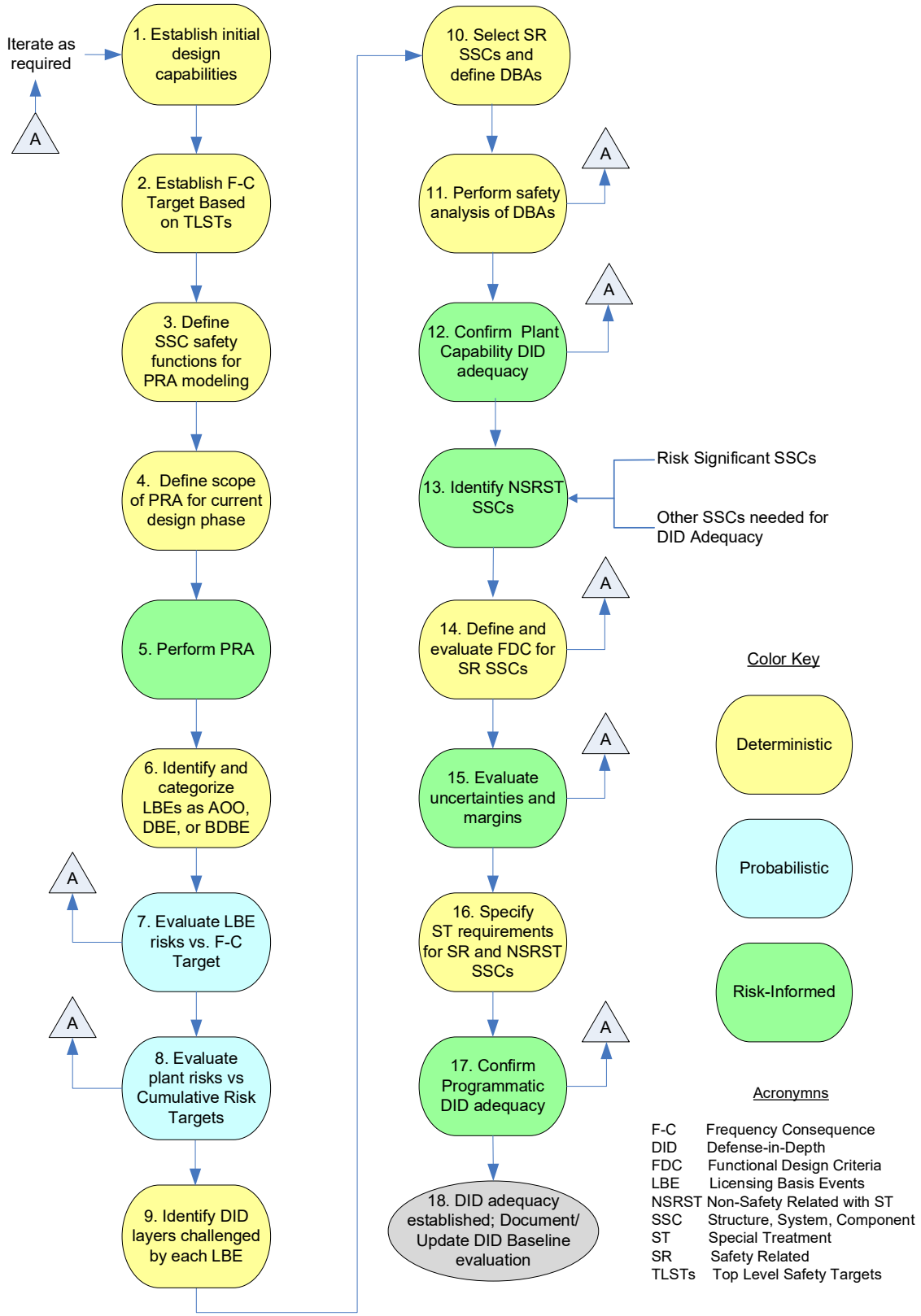

Figure 16. Integrated Process for Incorporation and Evaluation of Defense-in-Depth

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

The risk-informed and performance-based DID adequacy assessment is divided into eight tasks:

- Task 1. Establish Initial Design Capabilities
- Task 2. Establish Frequency-Consequence Target Based on Regulatory Objectives and Quantitative Health Objectives
- Task 3. Define SSC Safety Functions for Probabilistic Risk Assessment Modeling
- Task 4. Define Scope of Probabilistic Risk Assessment for Current Design Phase
- Task 5. Perform Probabilistic Risk Assessment
- Task 6. Identify and Categorize Events as AOOs, DBEs, or BDBEs
- Task 7. Evaluate Licensing Basis Event Risks vs. Frequency-Consequence Target
- Task 8. Evaluate Plant Risks vs. Cumulative Risk Targets

Task 1. Establish Initial Design Capabilities

The KP-FHR is a U.S.-developed Generation IV advanced reactor technology that has been developed over the last few years. This new reactor concept benefited from previous DOE-sponsored research and development activities conducted at universities and national laboratories. The fundamental concept is the combination of tri-structural isotropic (TRISO) particle fuel coupled with molten fluoride salt coolant. This combination results in a high-temperature, low-pressure reactor with robust, fully-passive safety systems.

In the last decade, U.S. national laboratories and universities have developed pre-conceptual Fluoride Cooled High Temperature Reactor (FHR) designs with different fuel geometries, power cycles, and power levels. Most recently, University of California, Berkeley developed the Mark 1 pebble-bed FHR, incorporating lessons learned from the previous decade of pre-conceptual designs. Kairos Power builds on the foundation laid by DOE-sponsored university Integrated Research Projects to develop the KP-FHR.

The fuel in the KP-FHR is the TRISO-coated particle fuel, originally developed for high-temperature gas-cooled reactors, which can withstand fuel particle temperatures up to 1,600°C before significant radionuclide release. The reactor coolant is the chemically stable, low-pressure molten fluoride salt mixture, 2LiF:BeF2 (flibe), with a boiling point of 1,430°C, notably lower than the 1,600°C fuel limit and yet functionally very high when compared to the operating temperature range. The combination of extremely high-temperature-tolerant fuel and low-pressure, single-phase, chemically stable reactor coolant removes entire classes of potential fuel-damage scenarios, greatly simplifying the design and reducing the number of required safety systems. The intrinsic low pressure of the reactor and associated piping, along with the functional containment provided by the TRISO fuel, enhances safety and eliminates the need for high-pressure containment structures.

A key measure of safety is the magnitude of the potential source term associated with off normal events. The source term represents the amount, timing and nature of the radioactive material released from the reactor core and available for release to the environment following a postulated accident. The KP-FHR design relies on a functional containment approach similar to the Modular High Temperature Gas-Cooled Reactor to meet 10 CFR 50.34 (10 CFR 52.79) offsite dose requirements at the plant's EAB with margin. A functional containment is defined in NRC Regulatory Guide 1.232 as a "barrier, or set of barriers taken together, that effectively limit the physical transport and release of radionuclides to the environment across a full range of normal operating conditions, anticipated operational occurrences (AOOs), and accident conditions." For the KP-FHR, the functional containment approach controls radionuclides primarily at their source within the coated TRISO fuel particle without requiring active design features or operator actions. The multiple barriers within the TRISO fuel particles and fuel pebble ensure that the dose at the EAB as a consequence of normal operations, AOOs, and design basis accident conditions meets regulatory limits. Additionally, the KP-FHR molten salt coolant also serves as a barrier providing retention of fission products that escape the fuel particle and fuel pebble barriers. These retention features are a key feature of the enhanced safety and reduced source term in the KP-FHR.

KP-FHR is both a low-pressure and physically compact reactor. The inherent safety of the KP-FHR technology also results in fewer safety-related systems, reducing the burden on design and inspection during the construction phase. The KP-FHR design facilitates off-site fabrication and assembly, reducing the expense of custom on-site fabrication and associated inspection.

Task 2. Establish Frequency-Consequence Target Based on Regulatory Objectives and Quantitative Health Objectives

Task 2 describes the approach for establishing an F-C Target based on regulatory objectives and quantitative health objectives. Two risk targets are described:

- F-C Targets
- Cumulative risk metrics

Frequency-Consequence Target

The PRA provides distributions for both the frequencies and consequences of all LBEs. The distributions for both frequency and consequence reflect a combination of the level of model uncertainty, design uncertainty, and data parametric uncertainty associated with that LBE.

The F-C Target curve presented in NEI 18-04 is used as a tool to analyze the KP-FHR's licensing basis events. Figure 17 shows the three general regions in which licensing basis events might fall on the frequency-consequence chart. The first is the region of low frequency and low consequence, where the event frequencies are always more than 100 times smaller than the target line. Events in this region are not risk-significant. The second region is denoted in the figure with horizontal lines and represents events that are considered risk-significant, but still acceptable against the target line. The third and final region of the frequency-consequence chart lies above the target line. Events in this region are considered risk-significant and in excess of the target.

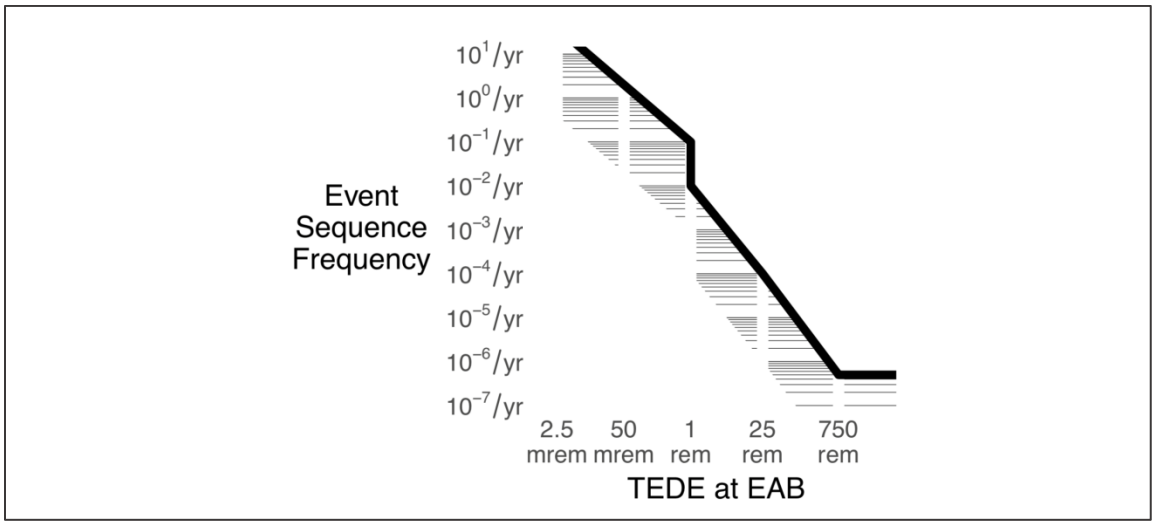

Figure 17. Frequency-Consequence Target Curve

Licensing basis events are represented on the frequency-consequence chart using six quantities from the PRA:

- Mean frequency of the event sequence occurring
- Uncertainty in the frequency calculation characterized by 5th and 95th percentiles
- Mean 30-day dose at the exclusion area boundary
- Uncertainty in the dose calculation characterized by 5th and 95th percentiles

Cumulative Risk Metrics

The cumulative risk metrics of the KP-FHR are also analyzed using the criteria from NEI-18-04.

- The total frequency of exceeding a site boundary dose of 100 mrem from all licensing basis events should not exceed 1/year. This metric is introduced to ensure that the consequences from the entire range of licensing basis events 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 licensing basis events shall not exceed 5×10^{-7}/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 Exclusion Area Boundary from all licensing basis events shall not exceed 2×10^{-6}/year to ensure that the NRC Safety Goal QHO for latent cancer fatality risk is met.

Task 3. Define SSC Safety Functions for PRA Modeling

The following safety functions are used in the PRA for all sources of radionuclides within the KP-FHR design:

- Control reactor power
- Control vessel temperature
- Control removal of decay heat
- Control radionuclide material

These required safety functions are deconstructed into specific safety functions in the PRA that take into account the conditions of the initiating event group and event sequence information.

Mitigation of AOOs and Prevention of DBEs

The following functions mitigate the consequences of the anticipated loss of flow and reduce the frequency of the design basis loss of flow:

- Normal reactor shutdown system detects the loss of flow and inserts non-safety control rods.
- Normal shutdown cooling system removes decay heat.

Both of these systems have capability targets to fulfill their mitigation function in response to the anticipated loss of flow. Both of these systems also have reliability targets such that events where the system is unavailable to perform its function, which would be a design basis loss of flow, are rarer than 10^{-2}/year.

Mitigation of DBEs and Prevention of BDBEs

The following functions mitigate the consequences of design basis loss of flow and, along with the non-safety functions listed above, reduce the frequency of beyond design basis loss of flow events:

- Safety reactor shutdown system initiates a reactor scram if a delay in the normal reactor shutdown occurs.
- Safety RVACS removes decay heat if the normal shutdown cooling system fails to maintain reactor temperatures within acceptable limits.

As above, both of these systems have capability targets to fulfill their mitigation function in response to the design basis loss of flow.

Both of these systems also have reliability targets such that events where the system is unavailable to perform its function, which would be a beyond design basis loss of flow, are rarer than 10^{-4}/year.

Mitigation of BDBEs and Prevention of Residual Risk Events

The following functions mitigate the consequences of beyond design basis loss of flow events and, along with the non-safety and safety-related functions above, reduce the frequency of residual risk events:

- Equipment used by operators to manually initiate a reactor control rod trip, or equipment used to repair failures of non-safety-related or safety-related control rods.
- Equipment used by operators to manually initiate decay heat removal which did not actuate automatically, or equipment used to repair failures of normal shutdown cooling or RVACS.

Both of these sets of equipment have capability targets to fulfill their mitigation function under the conditions defined by the beyond design basis loss of flow event. The conditions of the beyond design basis loss of flow events will be defined by the failure modes of the safety-related SSCs, which will be analyzed when detailed design information is available.

Both of these systems also have reliability targets such that events where the equipment is unavailable to perform its function, which would be a residual risk event eliminated from the licensing basis, are rarer than 5×10^{-7}/year.

Task 4. Define Scope of Probabilistic Risk Assessment

This task is an overlap between Step 3 of licensing basis event selection and Task 4 of DID adequacy.

A PRA has been introduced in the pre-conceptual design phase for the KP-FHR. The level of detail of the assessment is defined largely at the plant and system architectural levels, reflecting high-level success criteria and reliability information based on design targets and requirements.

The current scope of the PRA is characterized by the following:

- The at-power plant operating state is the initial focus of the risk assessment. This includes all plant challenges possible during power-delivery. All modes will be incorporated as operational design information matures.
- Internal events, including mechanical, human, fire, and flood hazards are within scope of the risk assessment. These hazards are studied at the plant-level and lean heavily on screening based on equipment separation requirements. External hazards such as external flood, seismic, and high winds will be incorporated as the site envelope characterization for the KP-FHR matures.
- System reliability is modeled by incorporating design reliability targets for individual and common mode failures. To characterize the reliability targets for yet-designed plant features, wide probability distributions are used to ensure that inherent design uncertainty is reflected in results.
- Success criteria, source term, and radiological consequences are defined in terms of retention requirements for radionuclide barriers. Similar to the system reliability figures, the uncertainty of yet-designed plant features is treated with wide probability distributions to ensure that the final results characterize the state of knowledge for the design.

The PRA has the following outputs relevant to licensing basis event selection and defense-in-depth adequacy:

- Definition of event sequence families
- Frequency calculations for event sequence families
- Consequence calculations for event sequence families

Task 5. Perform Probabilistic Risk Assessment

This task is an overlap between Step 3 of licensing basis event selection and Task 5 of defense-in-depth adequacy.

The PRA uses initiating event groups to treat initiators that have common challenges to reactor systems. The following is a summary of a few of the initiating event groups that are defined for the KP-FHR:

- The loss of forced core flow initiating event group subsumes all initiating event causes which cause core flow to be reduced during at-power operation. This group specifically excludes events that are associated with physical loss of primary coolant. The loss of core flow event features challenge to temperature limits on the TRISO fuel by dramatically increasing the power-to-flow ratio within the core. Additionally, this event may present challenges to the vessel structure due to a rapid thermal transient. Finally, the loss of core flow may also result in reduced heat removal capability from the primary salt. The increase in primary salt temperature is a challenge to the fission product solubility of the salt as a radionuclide barrier.
- The general transient initiating event group provides a group that can collect minor operational transients which may cause a reactor shutdown to correct a condition. This group specifically excludes events that are led by a total loss of core flow. Any transient initiating a shutdown presents a number of challenges to radionuclide barriers. First, the temperatures of the TRISO and vessel wall structures must be managed during the thermal transients associated with reducing power, whether rapid or slow. Second, any general transient where control rods are inserted present an opportunity to add a heat load to the primary salt, which could impact its fission product solubility for the circulating activity that is normally in the coolant.
- The loss of primary coolant initiating event group subsumes all initiating event causes which lead to a reduction in the primary salt inventory. The loss of primary coolant presents a challenge to TRISO fuel and vessel structures by nature of the rapid temperature transient these structures are subjected to. Additionally, this event may present cooling challenges to the primary coolant, which normally has a load of radionuclides in circulating activity.
- The KP-FHR has other initiating event groups that are not presented in this example.

To identify initiating events for the loss-of-flow event group, the hierarchical functional systems subsystem initiating event relationship [15, pp. 35–38] shown in Figure 3 was developed.

Hierarchical functional system subsystem initiating event relationships provide a systematic approach for the identification of initiating events in compliance with the Standard's requirements [11]. These diagrams are a precursor to the development of master logic diagrams; both diagrams provide a top down functional description of the system while the master logic diagrams would extend this model to explicitly account for system redundancy and dependency.

These relationship diagrams are developed via a top down approach where the Required Safety Functions are listed at the top of the diagram. The KP-FHR derivative safety functions exist in the second layer of the diagram. The systems that are responsible for achieving a given safety function are enumerated in the third layer of the diagram. Subsystems that impact a given Systems ability to achieve a Safety Function are listed in the fourth row. If component level information is available, it would comprise the next layer of the diagram. Depending of the level of design fidelity available, initiating events that could impact the lowest system or component are enumerated for that subsystem or component. This approach allows for a systematic, structured, and traceable mapping of initiating events that could impact the facility's ability to achieve the desired safety function.

The types of initiating events that belong to this loss of forced flow initiating event group are summarized in the bottom row of in Figure 3.

A simplified block diagram separating the levels of safety functions for the KP-FHR is shown in Figure 5.

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

This task in the DID assessment overlaps with Step 4 in licensing basis event selection.

The event sequences modeled and evaluated in the PRA are grouped into accident families each having a similar initiating event, challenge to the safety functions, plant response, end state, and mechanistic source term if there is a radiological release. Each of these families is assigned to an LBE category based on mean event sequence frequency of occurrence per plant-year summed over all the event sequences in the LBE family. The event families from this task are matched to the initial events generally described in Task 1.

The event sequence families from the PRA are described in the sections below. They are labeled with the event classification that matches both the product goals and the following frequency criteria from NEI 18-04:

- Anticipated operational occurrences have mean frequencies exceeding 10^{-2}/year.
- Design basis events have mean frequencies that do not exceed 10^{-2}/year to ensure that they are not anticipated in the lifetime of a single plant.
- Beyond design basis events have mean frequencies that do not exceed 10^{-4}/year to ensure that they are not anticipated in the lifetime of a fleet of plants.
- Residual risk events are excluded from the list of licensing basis events and have mean frequencies that do not exceed 5×10^{-7}/year.

Task 7. Evaluate Licensing Basis Event Risks vs. Frequency-Consequence Target

This task in the DID assessment overlaps with Steps 7a and 7c in licensing basis event selection.

This demonstration explains four licensing basis events:

- Anticipated loss of flow, LOF-AOO-1, which is a challenge for normal reactor shutdown and shutdown cooling systems
- Design basis loss of flow, LOF-DBE-1, which is a challenge for safety reactor shutdown and RVACS decay heat removal systems
- LOF-BDBE-1, which defines the beyond design basis challenge for the plant to recover from degraded decay heat removal
- LOF-BDBE-2, which defines the beyond design basis challenge for the plant to recover from an initial failure of normal and safety reactor shutdown systems

When plotted on the frequency-consequence chart with uncertainties (see Figure 6 through Figure 9), all of these licensing basis events have acceptable risk, and none are characterized as risk-significant.

Task 8. Evaluate Plant Risks Against Cumulative Risk Targets

This task in the DID assessment overlaps with Steps 7b and 7c in licensing basis event selection.

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

- The average individual risk of early fatality within 1 mile of the EAB from all LBEs shall not exceed 5×10^{-7}/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}/year to ensure that the NRC Safety Goal QHO for latent cancer fatality risk is met.
- 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.

Evaluation of Quantitative Health Objectives

The quantitative health objectives give targets for acceptable prompt and latent health risk. These measures are calculated for individual licensing basis events as well as for the total integrated plant risk.

The PRA provides distributions for consequences that include measures of both prompt and latent health risk. The distributions in each direction are sized reflecting a combination of the level of model uncertainty, design uncertainty, and data parametric uncertainty.

For consistency with the frequency-dose approach explained in Figure 1, health risk is also displayed on a frequency-consequence chart. This chart, shown in Figure 18, plots the frequency of an LBE against the conditional probability of a resulting health effect. The diagonal limit line represents a constant value for the product of frequency and consequence. (This is a feature of a chart with logarithmically distributed axes, where the product of the two quantities are constant along a diagonal line.) The frequency-consequence chart of health effects uses six quantities from the PRA.

- Mean frequency of the event sequence occurring
- Uncertainty in the frequency calculation characterized by 5th and 95th percentiles
- Mean conditional probability of a resulting health defect (either prompt or latent)
- Uncertainty in the conditional probability calculation characterized by 5th and 95th percentiles

This exercise is used to evaluate the integrated plant risk as well as to separate plant risk by LBE.

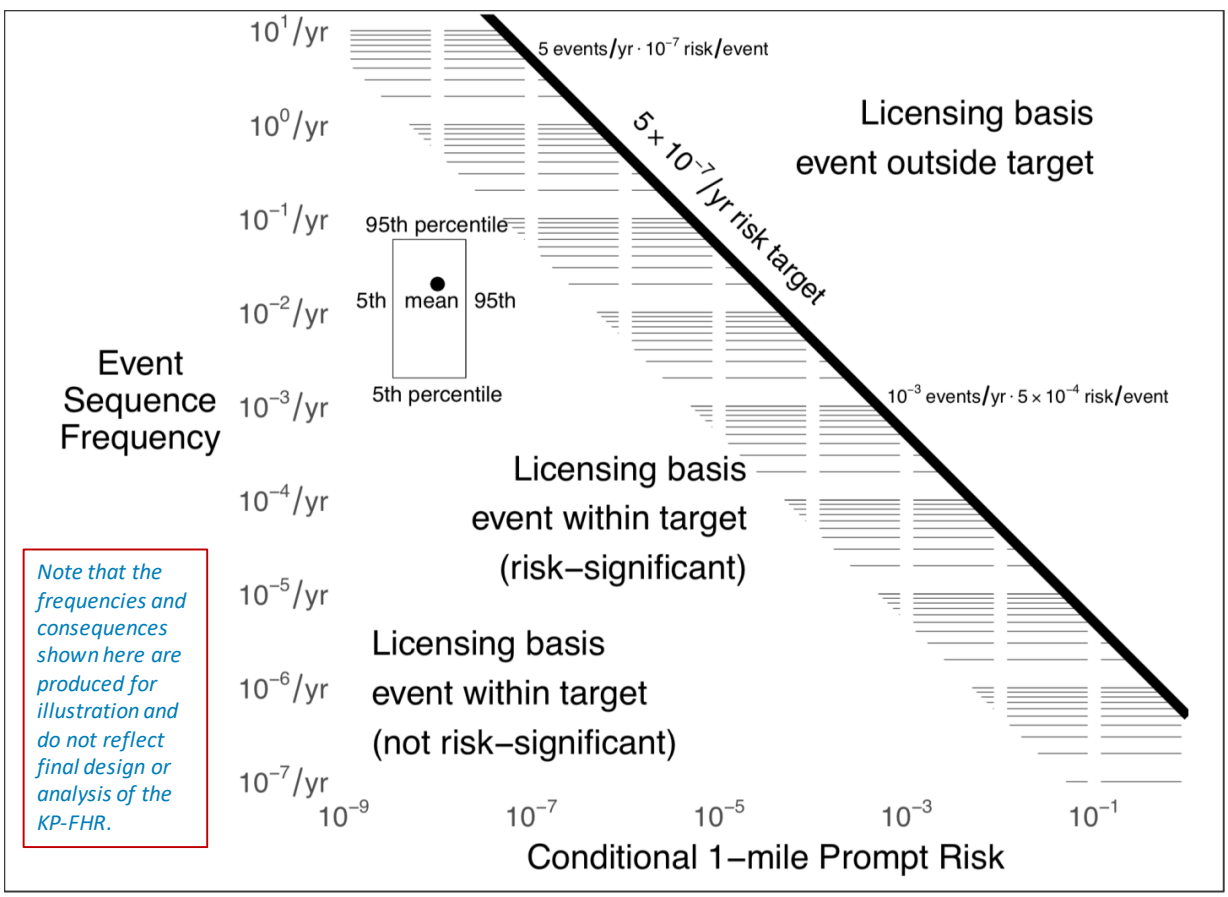

Figure 18. Example of Prompt Health Risk of Licensing Basis Event Against a Target

The conditional 1-mile prompt health risk and the 10-mile latent health risk were each plotted for each of the LBEs. Accounting for the uncertainty, as shown in the example of Figure 17, all health risks for all of the LBEs fell well within the "not risk-significant" area of the graphs.

Evaluation of 10 CFR 20 Risk

This task will be completed when a PRA of sufficient scope and capability is available to support it, including a complete set of event sequences, operating states, and hazard groups.

In lieu of a complete demonstration against this metric at this time, the event sequences which may exceed 100 mrem at the site boundary have their frequencies totaled in Figure 19. The frequency of exceeding 100 mrem at the boundary is a factor of one million smaller than the target, based on the design targets of the KP-FHR.

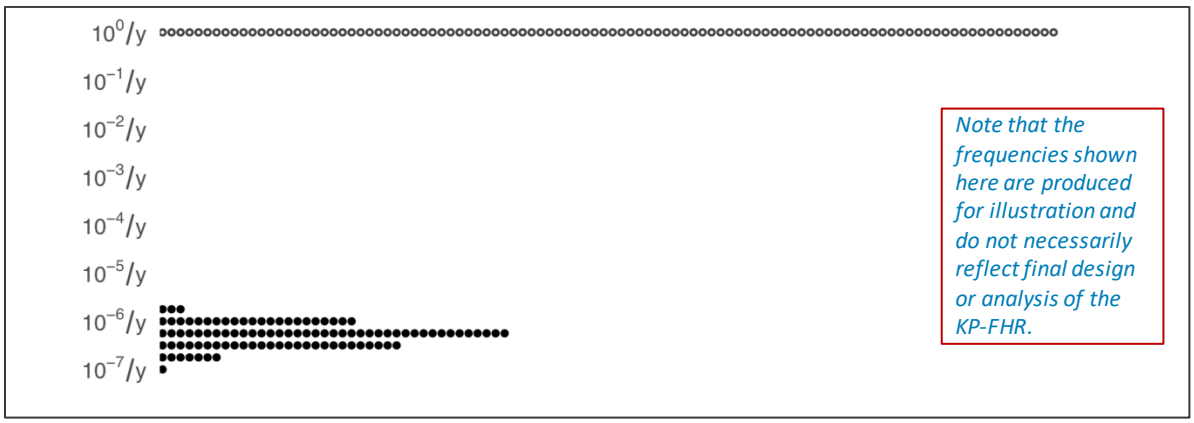

Figure 19. Frequency of Exceeding 100 mrem at Site Boundary for Loss of Flow Events

5.2 Evaluation of Plant Capability Defense-in-Depth

The plant capability DID adequacy assessment is divided into five tasks:

- Task 9. Identify DID Layers Challenged by Each Licensing Basis Event
- Task 10a. Select Safety-Related SSCs
- Task 10b. Define Design Basis Accidents
- Task 11. Perform Safety Analysis of Design Basis Accidents
- Task 12. Confirm Plant Capability DID Adequacy

Task 9. Identify Defense-in-Depth Layers Challenged by Each Licensing Basis Event

The design of plant response to various initiators is subdivided into a classical layers-of-defense paradigm, as shown in Figure 11.

The first layer of defense is represented by the plant's normal resilience to upset conditions through inherent and active control features. For a loss of flow event, the ability of the primary

core circulation pumps to maintain a flow rate in steady-state is the first line of defense against release.

The second layer of defense is represented by the plant's response to a failure of the first layer of defense. This presents the initiating event that is referred to in this work as the anticipated loss of flow. This event presents a challenge to the non-safety-related front-line systems that are responsible for guaranteeing that the plant can be placed in a safe and stable condition following the initiating event.

The third layer of defense is represented by the failures of Layer 1 (initiating loss of flow) and Layer 2 (unavailability of one of the front-line systems). This is a challenge to one or more safety-related systems. Either the safety control rods are demanded to make the reactor subcritical after failure of the Normal Reactor Control Shutdown, or the safety-related RVACS system is actuated to remove decay heat after failure of Normal Decay Heat Removal. The end state of successful Layer 3 operation is a safe and stable condition.

The fourth layer of defense treats the rare case of concurrent failures of Layer 1 (initiator), Layer 2 (non-safety-related equipment), and Layer 3 (safety-related equipment). This is a beyond design basis event that is a challenge to systems and operator actions to recover failed functions under extreme conditions. The result of these events is not necessary a safe and stable condition, but is measured by the mitigation of radionuclide release.

The fifth and final layer of defense considers the failure of systems and operator actions to recover from failures of safety-related systems. These events may end in a release that is not actively mitigated, but is still passively mitigated by the inherent features of the plant. Such features include the low operating pressure which will limit the transmission of a source term, as well as the high-retention TRISO fuel and the radionuclide solvency of the primary coolant salt (flibe).

Task 10a. Select Safety-Related SSCs

Task 10a in the DID assessment overlaps with Steps 5a, 5b, and 6 in the licensing basis event selection. Safety-related SSC safety requirements will be discussed in this section and DBA definitions will be discussed in the next section.

This section defines the following safety functions for safety-related SSCs associated with mitigating loss of flow events:

- Control core reactivity
- Remove decay heat
- Maintain vessel integrity
- Maintain TRISO integrity

Control Core Reactivity

The following safety-related SSCs are designed to be available to automatically shut down the reactor following any of the design basis events:

- Reactor shutdown rods
- Shutdown rod release and drive mechanisms
- Instrumentation to detect the need for reactor shutdown (i.e. thermocouples, transducers)
- Logic equipment to translate instrument readings to shutdown signals
- Actuation equipment to release rods and/or drive rods into the core
- Support systems that ensure the availability of above
- Physical supports that secure the shutdown rods and drives

The success of this fundamental safety function is measured by the subcriticality of the reactor and timing.

Remove Decay Heat

The following safety-related SSCs are designed to provide the fundamental safety function of removing core decay heat from the reactor following any of the design basis events:

- RVACS, including physical water storage tanks, cooling panels, valves, and associated equipment
- Instrumentation to detect the need for decay heat removal (i.e. thermocouples)
- Logic equipment to translate instrument readings to actuation signals
- Actuation equipment to open water valves and activate RVACS
- Structural supports for cooling panels
- Support systems that ensure the availability of RVACS to provide a passive decay heat removal function
- Air/water heat exchanger in RVACS stacks
- Physical RVACS chimneys
- Air intake structures
- Free-standing supports separate RVACS from the reactor building

The success of this fundamental safety function is measured by salt temperature limits which are defined based on qualification temperatures of the TRISO fuel particles.

Maintain Vessel Integrity

The function to maintain vessel integrity also involves the use of the RVACS SSCs defined above. The function is defined separately because the success criteria to protect the vessel structure during accident conditions will have separate success criteria than the decay heat

removal function. This function also serves to ensure that the primary salt coolant continues to surround the fuel pebbles for additional radionuclide retention.

In addition to the RVACS equipment identified above, vessel integrity also relies on the following:

- Vessel supports stabilizing the vessel in the cavity
- Cavity seals preventing water ingress into the reactor cavity

The success of this fundamental safety function is determined by temperature limits, stress limits, and environmental qualification conditions set by the design life constraints of the reactor vessel.

Maintain TRISO integrity

The consequences of all events with potential to release radionuclide material from the fuel are inherently limited by the assumed pre-transient conditions of the fuel. The fuel must therefore be monitored to provide high-confidence that the analysis conditions are not exceeded before the start of an accident.

The following safety-related SSCs are designed to ensure the pre-transient conditions of the TRISO fuel are within the analysis assumptions:

- Instrumentation to detect the radionuclide inventory of the reactor cover gas space
- Instrumentation to detect the radionuclide inventory of the circulating salt coolant
- Instrumentation to detect unexpected transient failures from fuel pebbles circulating in the pebble handling system

The success of this fundamental safety function is measured by assurance that conditions exceeding the analysis assumptions for pre-transient damage to TRISO particles are maintained during normal operation.

Task 10b. Define Design Basis Accidents

For each design basis event group identified in Step 4, a deterministic design basis accident is defined that includes the Required Safety Function challenges represented in the event, while also assuming that the Required Safety Functions are performed exclusively by safety-related SSCs and that all non-safety-related SSCs are assumed to be unavailable. These design basis accidents are also used in transient analysis of the license application for supporting the conservative deterministic safety analysis.

Loss of Flow Accident (LOF-DBA-1)

The design basis loss of flow (LOF-DBE-1) was defined in Step 1 and matched with the LOF-DBE-1 event sequence family from the PRA. In the design basis event, either the non-safety-related reactivity control system or the non-safety-related decay heat removal is unavailable. For

the design basis accident, both non-safety-related systems are unavailable because design basis events do not take credit for non-safety-related systems.

The following are characteristics of the loss of flow design basis accident (LOF-DBA-1):

- The reactor is operating at the most bounding power and flow steady-state condition before the onset of the transient.
- The burnup of the core is at the most limiting condition (likely end of life) for maximizing decay heat generation.
- The event begins with an abrupt loss of forced core flow.
- The safety-related reactor protection system detects the need to insert safety control rods through temperature or flow measurements within enough time to give margin to TRISO fuel temperature limits and vessel structural temperature limits.
- The safety-related RVACS eventually initiates according to the safety-related sensors and logic. This may include a delay timer depending on the final design of the RVACS. The timing and capacity of RVACS will give margin to TRISO fuel temperature limits and vessel structural temperature limits.
- A safe, stable state is reached when the reactor is subcritical and vessel temperatures have reached the threshold defined for safe shutdown.

Task 11. Perform Safety Analysis of Design Basis Accidents

This task in the DID assessment overlaps with Step 7d in licensing basis event selection.

This task corresponds to the traditional deterministic safety analysis that is found in the transient 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.

The deterministic safety analysis uses the following high level criteria [6] for design basis accident calculations:

- 10 CFR 50.34(a)(2)(ii)(D)(1) An individual located at any point on the boundary of the exclusion area for any 2 hour period following the onset of the postulated fission product release, would not receive a radiation dose in excess of 25 rem total effective dose equivalent (TEDE).
- 10 CFR 50.34(a)(2)(ii)(D)(2) An individual located at any point on the outer boundary of the low population zone, who is exposed to the radioactive cloud resulting from the postulated fission product release (during the entire period of its passage) would not receive a radiation dose in excess of 25 rem total effective dose equivalent (TEDE).

The description of the evaluation model and results of calculations are the subject of future work.

Task 12. Confirm Plant Capability Defense-in-Depth Adequacy

The adequacy of the KP-FHR's plant capability DID is given by examination of Tasks 9 through 11 in this work.

- Task 9. Identify DID Layers Challenged by Each Licensing Basis Event
- Task 10. Select Safety-Related SSCs and Define Design Basis Accidents
- Task 11. Perform Safety Analysis of Design Basis Accidents

The evaluation will focus on the following attributes of plant capability DID:

- 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

The evaluation also studies the following features from the "layers of defense" framework:

- Multiple Layers of Defense
- Extent of Layer Functional Independence
- Functional Barriers
- Physical Barriers

Functional reliability is another subject of the plant capability DID evaluation, focusing on the following:

- Inherent Reactor Features that contribute to performing PRA Safety Functions
- Passive and Active SSCs performing PRA Safety Functions
- Redundant Functional Capabilities
- Diverse Functional Capabilities

A critical part of the plant capability DID is the balance of prevention and mitigation of releases. The following are points of focus in this area:

- SSCs performing prevention functions
- SSCs performing mitigation functions
- No Single Layer / Feature Exclusively Relied Upon

Evaluation of this section is currently out of scope and will be completed when sufficient design detail is available to support the evaluation of safety-related structures system and components.

5.3 Evaluation of Programmatic Defense-in-Depth

The programmatic DID adequacy assessment is divided into five tasks:

- Task 13. Identify NSRST SSCs
- Task 14. Define and Evaluate Required Functional Design Criteria for SR SSCs
- Task 15. Evaluate Uncertainties and Margins
- Task 16. Specify Special Treatment Requirements for SR and NSRST SSCs
- Task 17. Confirm Programmatic DID Adequacy

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

This task in the DID assessment overlaps with Step 5a in licensing basis event selection. 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. 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 given 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.

- The total frequency of exceeding a site boundary dose of 100 mrem should not exceed 1/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 licensing basis events with the SSC failed is greater than 10^{-2}/year.
- The average individual risk of early fatality within 1 mile of the EAB shall not exceed 5×10^{-7}/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 licensing basis events with the SSC failed is greater than 5×10^{-9}/year.
- The average individual risk of latent cancer fatalities within 10 miles of the EAB shall not exceed 2×10^{-6}/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 licensing basis events with the SSC failed is greater than 2×10^{-8}/year.

Table 5 provides a summary of risk-significance and safety-significance formally discussed in the SSC classification report [3].

Table 5. Safety-Significance of Functions

Function	Risk-Significant	Needed for DID
Non-safety-related reactivity control	No	Yes
Beyond design basis reactor control	No	Yes
Non-safety-related decay heat removal	No	Yes
Beyond design basis decay heat removal	No	Yes

The SSCs supporting each function are identified in the sections below.

Defense Layer 2 Reactivity Control

The non-safety-related reactivity control equipment includes the following:

- Non-safety reactor control rods
- Control rod release and drive mechanisms
- Instrumentation to detect the need for reactor control (i.e. thermocouples, transducers)
- Logic equipment to translate instrument readings to shutdown signals
- Actuation equipment to release rods and/or drive rods into the core
- Support systems that ensure the availability of above
- Physical supports that secure the control rods and drives

Defense Layer 4 Reactivity Control

The beyond design basis equipment for the reactivity control function includes:

- Control room or reactor building equipment used by operators to manually recover from a failure to scram automatically
- Structures that protect manways or operator access to critical control rod equipment to perform beyond design basis repair procedure actions
- Instrumentation and control systems that are critical to diagnosing failures

Defense Layer 2 Decay Heat Removal

The non-safety-related normal shutdown cooling equipment includes the following:

- Normal shutdown cooling piping, heat exchangers, and ultimate heat sink equipment
- Instrumentation to detect the need for decay heat removal (i.e. thermocouples)
- Logic equipment to translate instrument readings to actuation signals
- Actuation equipment to actuate normal shutdown cooling
- Structural supports for piping, heat exchangers, and ultimate heat sink equipment
- Support systems that ensure the availability of normal shutdown cooling to provide the decay heat removal function

Defense Layer 4 Decay Heat Removal

The beyond design basis equipment for decay heat removal function include:

- Structures that protect manways or operator access to critical RVACS equipment to perform beyond design basis repair procedure actions
- Instrumentation and control systems that are critical to diagnosing failures

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

Required functional design criteria provide a bridge between the design basis accidents and the formulation of design criteria for the safety-related SSCs. DID attributes such as redundancy, diversity, and independence, and the use of passive and inherent means of fulfilling Required Safety Functions are used in the formulation of required functional design criteria.

The first priority in establishing the design targets 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 structure, system, or component are sufficiently defined for all the functions represented in the licensing basis events. A related priority is to provide reasonable confidence that the reliability and capability of the SSCs are achieved and maintained throughout the lifetime of the plant.

Those SSCs that are classified as safety-related are expected to meet applicable regulatory requirements as well as reactor-specific and design-specific safety-related design criteria derived from the required functional design criteria.

The following tasks will be performed as part of future work to determine the required capabilities for each piece of safety-significant equipment:

- Determine safety-related design criteria for safety-related SSCs to perform required safety functions
- Determine non-safety-related SSC reliability and capability targets to perform safety-significant functions

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

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 licensing basis events in which the SSC performs a safety-significant function. The magnitudes of the safety margins in performance are set considering the uncertainties in performance, the nature of the associated licensing basis events, 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 licensing basis events.

A second example of the use of margins is in the selection of reliability performance targets. The reliability targets are set so that the underlying LBE frequencies and consequences with uncertainties meet the LBE evaluation criteria with 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 licensing basis events and the F-C Target and the margins between the cumulative risk metrics and the cumulative risk targets used for licensing basis event evaluation. These risk margins are assessed as part of the risk-informed performance-based evaluation of DID.

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 reasonable assurance that the SSCs will be capable of performing their PRA Safety Functions with appropriate margins for uncertainties and with an appropriate degree of reliability. These include numerical targets for SSC reliability and availability, design margins for performance capability of the PRA Safety Functions, and monitoring of performance against these targets with appropriate corrective actions when targets are not fully realized. Another consideration in the setting of SSC performance requirements is the need to assure that the results of the plant capability DID evaluation in Step 12 are achieved not just in the design, but in the as-built and as-operated and maintained plant following manufacturing and construction, and maintained during the life of the plant. The SSC performance targets are set or confirmed during the design integrated decision-making process that is responsible for establishing the adequacy of DID. In addition to these performance targets, special treatments may be identified to address safety-significant performance uncertainties.

Task 17. Confirm Programmatic Defense-in-Depth Adequacy

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

When the programmatic defense-in-depth adequacy assessment is completed in its final form, the following quality and reliability items will be validated:

- Performance targets for SSC reliability and capability
- Design, manufacturing, construction, O&M features, or special treatment sufficient to meet performance targets

The programmatic DID assessment will also comment on the adequacy of uncertainty compensation, including for the following:

- Compensation for human errors
- Compensation for mechanical errors
- Compensation for unknowns (performance variability)
- Compensation for unknowns (knowledge uncertainty)

Additionally, the need for and adequacy of offsite emergency response capability will be assessed.

Evaluation of this section is currently out of scope and will be completed when sufficient design detail is available to support this evaluation.

5.4 Summarize the Adequacy of Defense-in-Depth

Task 18. Defense-in-Depth Adequacy Established

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

The successful outcomes of Tasks 12, 17 and 18 establish DID adequacy. This determination is made incrementally during the Integrated Decision Process and documented progressively in a DID integrated baseline evaluation report which is subsequently revised as the iterations through the design cycles and design evaluation evolve. In task 18, the integrated evaluation of DID adequacy confirms the attributes of DID have been addressed for:

- Plant Capability DID Adequacy
- Programmatic DID Adequacy
- Risk-Informed and Performance-Based DID Adequacy

While some portions of DID cannot be confirmed given the current level of design detail associated with the KP-FHR, system reliability targets allow the KP-FHR to confirm that DID is adequately provided on the system level for Loss of Flow AOOs, DBEs, and BDBEs.

6.0 CONCLUSIONS AND OBSERVATIONS

6.1 Conclusions

The Demonstration Project met the objectives and deliverables as outlined in the project charter and summarized in this report.

Objective 1 Conclusions

Objective 1: Demonstrate key processes within the LMP Guidance Document applied to the KP-FHR.

Significant progress was made to demonstrate the selection of LBEs based on information obtained from the KP-FHR PRA for event sequences, combined with performance-based targets for frequency and radiological dose, reflecting the KP-FHR pre-conceptual design and additional efforts to estimate offsite radiological doses for each LBE. The process of defining the required safety functions using KP-FHR examples was also demonstrated. Options for selecting safety-related SSCs for each required safety function were identified in these examples. However, it should be noted that classification of SSCs as safety-related will ultimately be made by the designer. The process of evaluating DID adequacy was also reviewed.

Based on the scope and design basis of this Demonstration Project, the process described in the LMP Guidance Document was shown to provide a systematic and reproducible framework for selection of LBEs, defining required safety functions, classification of SSCs, and the process for evaluating the adequacy of defense-in-depth.

Objective 2 Conclusions

Objective 2: Leverage the LMP process to improve the regulatory certainty of Kairos Power's FHR design and safety case, as best possible at the current state of design, by identifying a credible spectrum of Licensing Basis Events and investigating available SSC groupings that result in acceptable outcomes for the identified LBEs. Underlying this objective is the assertion that use of risk informed, performance based methods to reach these conclusions are endorsed by Commission policy and compatible with the existing regulatory framework.

The Demonstration provided insights into how the technology-inclusive, RIPB LMP process can be incorporated during the pre-conceptual design and subsequent phases of the KP-FHR by providing a process to reduce regulatory uncertainty; specifically, in the areas of LBE selection, identification of required safety functions, SSC classification, and DID adequacy.

It is expected that the LMP Demonstration Project, and this associated report, will serve as an input into Kairos Power's regulatory engagement strategy. Additionally, some important safety design questions were raised as part of the Demonstration which is one of the objectives of the LMP methodology. While no decisions were made during this Demonstration, an understanding of the RIPB processes proved valuable in identifying the steps needed to evaluate the safety-risk associated with various design selections and the tradeoffs needed from other stakeholders to achieve broader designer objectives.

One example of a design selection is the selection of SR SSC sets. An initially selected SR SSC may change after the LMP process is performed given some newly identified options for satisfying the required safety functions. This selection then becomes a design requirement on those new or modified SSCs. Those SSCs must have a certain design maturity, based on a list of initial functions and requirements, to base at least a preliminary-level PRA, like the pre-conceptual KP-FHR PRA. This process highlighted some iterative design steps which may occur as a result of performing the LMP processes.

In summary, this Demonstration shows the LMP processes have the potential to reduce regulatory uncertainty by providing a systematic and transparent process, as well as criteria, for addressing key and fundamental safety questions and informing design decisions.

6.2 Observations

- For the LMP to be fully effective, organizations should provide internal training on the LMP process, and ensure the appropriate members are sufficiently involved.
  - Decision makers beyond the core engineering staff should use/embrace and be sufficiently knowledgeable of the LMP process to ensure regulatory/licensing success.
  - It is important for the licensing team following the LMP approach to have key engineering design team members and decision makers in charge of the safety function development and the selection of SSC safety classification involved in the execution of the LMP methodology.
- LMP provides a RIPB framework for making decisions that impact the safety design approach and technical basis for licensing activities. Based on the Demonstration, Kairos Power feels like the usefulness and benefits of the LMP RIPB process will increase over time as the design completion/PRA update integration processes are performed.
- The LMP approach to functional design criteria can satisfy the requirement for identification of Principle Design Criteria. Additional effort is needed to define the relationship of the LMP process with Advanced Reactor Design Criteria, and other licensing requirements. These are topics currently being discussed as the Guidance Document and associated NRC interactions move forward.
- RIPB decisions in the LMP framework are made by the designer (e.g. by an integrated decision-making panel, or equivalent) to achieve a safe, practical design that can be presented for approval by the regulator. This exercise of the LMP framework initially demonstrated that the RIPB processes can successfully:
  - Provide a process for selecting and evaluating LBEs including the selection of DBAs driven by user selected safety-related SSCs for the performance of required safety functions.
  - Provide criteria for establishing risk-significant and safety-significant SSCs. Based on insights from the KP-FHR Demonstration and previous HTGR examples, it is likely that for Kairos Power's KP-FHR, most risk-significant SSCs will be contained within

the set of safety-related SSCs because none of the SSCs beyond the SR SSCs are expected to meet the LMPs criteria for risk-significance.

  - Enable the designer to establish requirements for the SSC reliabilities and capabilities to prevent and mitigate LBEs that will flow down to the special treatment requirements for safety-significant (SR and NSRST) SSCs.
  - Give the designer ownership of the responsibility to evaluate the adequacy of DID whose documentation will be available for review and audit by the NRC.
  - The Guidance Document provides flexibility to the designer to meet other top-level requirements (e.g. performance, cost, risk, etc.).

- As DID adequacy evaluations are finalized, programmatic actions to assure reliability and performance requirements (e.g. technical specifications, reliability assurance programs, limits of operation, surveillance requirements, etc.) can be completed for all the SR and any NSRST SSCs. Margin to the F-C Target, including uncertainty analysis, can lead to the derivation of less stringent performance requirements than what has been typically done for existing light water reactors.

7.0 REFERENCES

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

[2] "Licensing Basis Event Selection," Kairos Power (Proprietary), KP-NSA-001, Rev. 0, April 2019.

[3] "Safety Classification of Structures, Systems, and Components," Kairos Power (Proprietary), KP-NSA-002, Rev. 0, April 2019.

[4] "Defense-in-Depth Evaluation," Kairos Power (Proprietary), KP-NSA-003, Rev. 0, April 2019.

[5] Idaho National Laboratory, "Next Generation Nuclear Plant Probabilistic Risk Assessment White Paper," INL/EXT-11-21270, ADAMS Accession Number ML11265A082, September 2011.

[6] "Contents of applications; technical information." https://www.nrc.gov/reading-rm/doc-collections/cfr/ part050/part050-0034.html; U.S. Nuclear Regulatory Commission, 10 CFR 50.34.

[7] Idaho National Laboratory, "Modernization of Technical Requirements for Licensing of Advanced Non-Light Water Reactors, Probabilistic Risk Assessment Approach," August 2019.

[8] Idaho National Laboratory, "Modernization of Technical Requirements for Licensing of Advanced Non-Light Water Reactors, Selection and Evaluation of Licensing Basis Events," August 2019.

[9] Idaho National Laboratory, "Modernization of Technical Requirements for Licensing of Advanced Non-Light Water Reactors, Safety Classification and Performance Criteria for Structures, Systems and Components," August 2019.

[10] Idaho National Laboratory, "Modernization of Technical Requirements for Licensing of Advanced Non-Light Water Reactors, Risk-Informed and Performance-Based Evaluation of Defense-in-Depth Adequacy," August 2019.

[11] American Society of Mechanical Engineers and American Nuclear Society, "Probabilistic Risk Assessment Standard for Advanced Non-LWR Nuclear Power Plants," ASME/ANS RA-S-1.42013, December 2013.

[12] U.S. Nuclear Regulatory Commission, NUREG/KM-0009, "Historical Review and Observations of Defense-in-Depth," ADAMS Accession Number ML16104A071, April 2016.

[13] "An approach for using probabilistic risk assessment in risk-informed decisions on plant-specific changes to the licensing basis," https://www.nrc.gov/docs/ML1009/ML100910006.pdf; U.S. Nuclear Regulatory Commission, Reg. Guide 1.174, 2018.

[14] "Guidance on the treatment of uncertainties associated with PRAs in risk-informed decision making," https://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr1855/; U.S. Nuclear Regulatory Commission, NUREG-1855, March 2017.

[15] M. Modarres, Risk analysis in engineering: Techniques, tools, and trends. Taylor & Francis, 2006.

[16] Idaho National Laboratory, "Modernization of Technical Requirements for Licensing of Advanced Non-Light Water Reactors, High Temperature, Gas-Cooled Pebble Bed Reactor Licensing Modernization Project Demonstration," Revision 0, August 2018.

[17] "Guidance for a Technology-Inclusive, Risk-Informed, and Performance-Based Methodology to Inform the Licensing Basis and Content of Applications for Licenses, Certifications, and Approvals for Non-Light Water Reactors" (ML18312A242) U.S. Nuclear Regulatory Commission, Draft Reg. Guide DG-1353, May 2019.

From:	Afzali, Amir
To:	Segala, John; Cubbage, Amy; Reckley, William
Cc:	Jim C. Kinsey Jr; Wayne Moe (wayne.moe@inl.gov); Shirley, Barry J.; Peter Hastings; Jordan Hagaman
Subject:	[External_Sender] Kairos Power LMP Demo Report
Date:	Tuesday, September 03, 2019 9:26:47 PM
Attachments:	Kairos Power LMP Demonstration Report Rev 0 September 2019_signed.pdf

---

Greetings,

Please find attached Kairos Power's tabletop report. The LMP team is thankful to Kairos Power staff and management for supporting LMP activities and working with us to perform the expert work that resulted in this insightful report.

Best regards,

Amir

Amir Afzali
Southern Company Services
Licensing and Policy Director- Next Generation Reactors
Energy Center
Birmingham, AL 35242
Phone: (205) 992-5937
Mobile: (443) 912-3726

Southern Company