GIF-RSWG & WGSAR

Risk Informed Approach for Event Selection and Evaluation

Jim Kinsey
Idaho National Laboratory
Office of Nuclear Energy
U.S. Department of Energy

October, 2019

1

1

Overview of Oct. 2018 Proposal to WGSAR

- Develop a report summarizing a structured approach for the incorporation of risk insights when making facility safety assessments and regulatory decisions is proposed to supplement the deterministic approach, with the following expected benefits:
  - Increased confidence that key safety issues have been fully identified and addressed
  - Better understanding of safety margins
  - Facilitates more structured dialogue among international regulators
  - Reduced reliance on “expert judgement” through a rigorous, pre-defined process with more predictable outcomes
- Proposed outcome is development of a report summarizing the structure and key considerations for applying this approach that:
  - Is inclusive of advanced reactor technologies
  - Provides for flexible implementation recognizing unique and varying sovereign regulatory structures
  - Builds upon existing/current GIF safety approaches (e.g., GIF Basic Safety Approach, Integrated Safety Assessment Methodology)

2

2

High Level Objectives of Design Assessments and Regulatory Reviews

Based on regulatory requirements and associated implementing guidance, a designer's license application must typically answer the following questions:

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

3

3

Foundation Of This Proposed Approach

- The underlying foundation of this approach is that, if the risk of an event is defined as the product of the event's frequency of occurrence and its consequences, then the design of the plant should be such that all the AOOs and other more significant event sequences produce an acceptable level of risk when compared against regulatory requirements.
- To address this foundational concept, the identification and categorization of event sequences must be risk-informed, utilizing a blend of risk insights and deterministic inputs, in setting and assessing design targets.

Note: In April, 2017, the GIF-RSWG was briefed on the approach we'll discuss today. That briefing provided a summary of work being done within the IAEA Coordinated Research Project developing safety design criteria for modular HTGRs.

4

4

Proposed Approach - Outcome Objectives

This overall approach is intended to assist designers and regulators in understanding and addressing the overall facility response to a broad spectrum of events by addressing the following objectives.

1. Establish the concept of high-level regulatory criteria within each country's existing structure for protecting public health and safety. Summarize the basic event sequence types that must be addressed in design assessments and associated regulatory actions
2. Establish event-sequence evaluation as the approach that allows facility evaluation against the high-level regulatory criteria, including the option for assessing multi-reactor and multiple radionuclide source risk
3. Describe the structure of the frequency-consequence target as the foundation of the proposed risk-informed and performance based approach
4. Establish a structured risk-informed approach that can be repeatedly applied while achieving consistent results when blending the use of deterministic inputs and risk insights to identify and categorize events
5. Establish a process for deriving design specific required safety functions from the fundamental safety functions

5

5

Outcome Objectives (cont.)

6. Establish a process to effectively classify structures, systems, and components (SSCs), with the goal of focusing attention and resources on those SSCs that are most risk significant
7. Establish a process for the development of SSC performance requirements for preventing and mitigating releases, including both capability and reliability
8. Describe the conservative and deterministic assumptions applied to derive design-basis accidents (DBAs)
9. Describe key constituents of defense in depth (DID), including plant capability and programmatic aspects
10. Establish an approach for the use of expert judgment, combined with the use of risk insights, for assessing the adequacy of DID.

Note: It is recognized that this approach represents various process and terminology differences from the currently described approaches for GEN IV systems. Those differences will be discussed among the GIF and WGSAR stakeholders to determine how they can be integrated into existing approaches, or identified as open issues to be addressed outside of the planned report.

6

6

High Level Regulatory Criteria

7

7

Foundation for Evaluating Plant Margins of Safety in Support of Licensing & Public Protection

- **What** must be met:
  - High Level Regulatory Criteria (HLRC)
- **When** HLRC must be met:
  - Licensing Basis Events
- **How** HLRC must be met:
  - Safety Functions
  - SSC Safety Classification
- **How well** HLRC must be met:
  - Deterministic DBAs
  - Defense-in-Depth
  - Regulatory Special Treatment

8

8

High Level Regulatory Criteria

- The term High Level Regulatory Criteria (HLRC) refers to limits on radiological releases for various plant events. This approach is chosen because HLRC are:
  - Generic, technology-neutral, and independent of plant site
  - Quantitative, and thereby useful in a performance-based context
  - Provide a direct statements of acceptable consequences or risks to the public
- In general, the HLRC are associated with event sequences (dose at the fence), rather than on initiating events; different event sequences following an initiating event have different frequencies and consequences
- It is noted that the HLRC structure is generally similar among member countries, although the specific terminology and release limits differ
- Application of the approach being described in this paper allows for the assessment of multi-reactor module risk for an entire facility, rather than being limited to an individual reactor basis

9

9

Event Sequence Evaluation

and

Structure of Frequency-Consequence Targets

10

10

Foundation for Evaluating Plant Margins of Safety in Support of Licensing & Public Protection

- **What** must be met:
  - High Level Regulatory Criteria (HLRC)
- **When** HLRC must be met:
  - Licensing Basis Events
- **How** HLRC must be met:
  - Safety Functions
  - SSC Safety Classification
- **How well** HLRC must be met:
  - Deterministic DBAs
  - Defense-in-Depth
  - Regulatory Special Treatment

11

11

Terminology Issues and Challenges

Key Terms Used in This Proposed Approach

Risk-Informed: An approach that includes a blend of risk insights and deterministic inputs

Licensing Basis Events (LBEs): Broadly defined to include all the events used to support the safety aspects of the design and to meet licensing requirements. They cover a comprehensive spectrum from normal operation to rare, off-normal event. (LBE categories are described on the next slide)

Fundamental Safety Functions: Generally considered to include: 1) retention of radionuclides, 2) control of core heat removal, 3) control of heat generation

Selected Terminology and Proposed Approach Content Requiring GIF-WGSAR Dialogue Going Forward

- Relating Plant States to the concept of Event Sequence
- Design Basis Event terminology and relation to AOOs and DBAs
- Design Extension Conditions
- Residual Risk Events and Practically Eliminated Accidents

12

12

Licensing Basis Event (LBE) Sequence Categories

Anticipated Operational Occurrences (AOOs) Anticipated event sequences expected to occur one or more times during the life of a nuclear power plant, which may include one or more reactor modules or sources. AOOs take into account the expected response of all SSCs within the plant, regardless of safety classification, to fully understand plant capabilities. However, safety grade systems are not relied on to provide an acceptable plant response and outcome from AOO event sequences.

Design Basis Events – Infrequent event sequences that are not expected to occur in the life of a nuclear power plant, which may include one or more reactor modules or sources, but are less likely than AOOs. DBEs are the basis for the design, construction, and operation of the structures, systems, and components (SSCs) during accidents and are used to provide input to the definition of design basis accidents (DBAs).

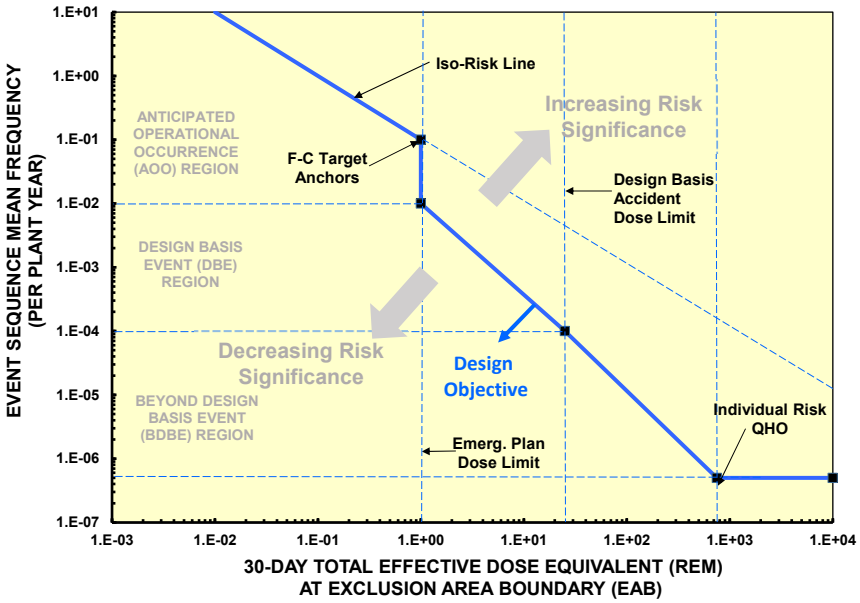
Beyond Design Basis Events (BDBEs): Very rare event sequences that are not expected to occur in the life of a nuclear reactor fleet, which may include one or more reactor modules or sources, are less likely than a DBE, but are still considered in the design. BDBEs take into account the expected response of all SSCs within the plant, regardless of their safety classification.

Design Basis Accidents (DBAs): Postulated event sequences that are less likely than AOOs and not expected to occur in the life of a nuclear power plant, which may include one or more reactor modules or sources, but are considered in the design. DBAs are used to set design criteria and performance objectives for the design of safety-related SSCs, since DBA response relies on only safety-related SSCs.

13

13

Example Frequency-Consequence Target Structure



14

14

Key Aspects of Frequency-Consequence Evaluation

- The frequency of event-sequence categories is evaluated on a per-plant-year basis, which allows for all reactors and radionuclide sources on a plant site to be evaluated in combination.
- The AOO, DBE, and BDBE event sequence categories are based on the mean event-sequence frequency of occurrence per plant-year.
- The regions of the figure separated by the frequency-dose evaluation line are identified as increasing and decreasing risk to emphasize that the purpose of the criteria is to evaluate the risk significance of individual AOOs, DBEs, and BDBEs, and to recognize that risk evaluations are not performed on a pass-fail basis, in contrast with deterministic safety evaluation criteria.
- Event sequences may or may not involve release of radioactive material and may involve two or more reactor modules or radionuclide sources.
- Across the entire spectrum of the F-C chart, the F-C target is selected such that the risk, defined as the product of the frequency and consequence, does not increase as the frequency decreases.
- It is expected that many LBEs will not result in the release any radioactive material, although they still assist in forming the basis for defining safety related SSCs

15

15

Repeatable Event Identification Approach

Task 1: Propose Initial List of Initiating Events and Resulting Event Sequences

It is necessary to select an initial set of LBEs that may not be complete, but are necessary to develop the basic elements of the safety design. These events are to be selected deterministically and may be supported by qualitative risk insights based on all relevant and available experience

Task 2: Design Development and Analysis

Design development is performed in phases and often includes a pre-conceptual-, conceptual-, preliminary-, and final-design phase and may include iterations within phases

Task 3: PRA Development/Update

A PRA model is developed and then updated as appropriate for each phase of the design. Prior to the first introduction of the PRA, it is necessary to develop a technically sound understanding of the potential failure modes of the reactor concept, how the plant would respond to such failure modes, and how protective strategies can be incorporated into formulating the safety design approach.

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

The event sequences modeled and evaluated in the PRA are grouped into event sequence families

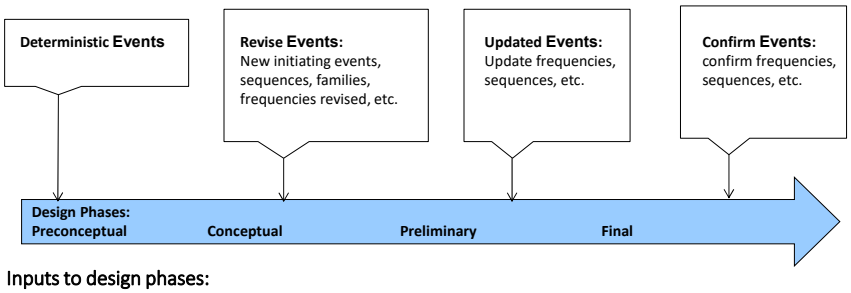
Each of these families is assigned to an event sequence category based on mean event-sequence frequency of occurrence per plant-year summed over all the event sequences in the family.

16

16

Design Development Timeline

Event evolution by design phase:



Inputs to design phases:

- Initial design concept
- Prior operating experience & PRAs
- Expert insights

- Basic design
- Initial analyses (PIRT, OPT, etc.)
- Prior operating experience
- Initiate PRA development
- Design rqmts.
- Expert reviews

- Updated design
- Detailed analyses, etc.
- Initial PRA results
- Expert reviews
- Regulator interaction

- Mature design
- Detailed analyses, etc.
- Complete PRA results
- Expert reviews
- Regulator feedback

17

17

PRA Development

- PRA is selected for use in systematic identification of initiating events and event sequences and for providing risk insights into risk-informed decisions
- Although not required, early introduction of PRA into the design process is encouraged and facilitates risk-informing design decisions
- Scope and level of detail is consistent with scope and level of detail of design and site information and fit for purpose in RIPB decisions
- Depending on the stage of the design, PRA event-sequences include those hazards that have state of practice PRA methods and involve single and multiple reactor modules and include risk significant non-reactor sources
- Limitations and uncertainties associated with PRA addressed in the evaluation of defense-in-depth adequacy and deterministic inputs to risk-informed and performance-based decisions

18

18

Establishing the Technical Adequacy of PRA

- ASME/ANS started the development of a non-LWR PRA standard in 2006 and produced a trial use standard ASME/ANS-Ra-S-1.4-2013
- Scope includes multiple operating states, all hazards, source terms and radiological consequences and sequences with multiple modules and sources
- Approximately 80% of the technical requirements are common to the LWR PRA standards; remaining 20% address:
  - Risk metrics appropriate for all advanced non-LWRs
  - PRAs on multi-module plants
  - PRAs that support event sequence frequencies and radiological consequences
  - PRAs that are performed at early stages in design
- Standard extensively tested in PRA pilots on pebble bed HTGRs, SFRs, MSRs, and Micro-reactors; Supported licensing of HTR-PM in China
- Standard used for PRAs in Licensing Modernization Project pilots for X-Energy Xe-100, GE-PRISM, MSRE, Kairos-FHR, and Westinghouse eVinci Micro Reactor
- Trial use standard is currently being revised towards a ballot for an ANSI standard in 2020
- NRC has supported the development of the standard, developing Interim Staff Guidance for use of 2013 version, and plans to endorse the 2020 version in a regulatory guide

19

19

Recent US Industry Experience

20

20

Recent US Experience in Applying the Approach

- Key parts of this approach have recently been assessed and demonstrated through a series of "pilot" studies in the US as part of an ongoing dialogue between reactor designers and regulators
- Those studies have included a broad range of GEN IV technologies
- Example results will now be presented for information
- More information can be found in the specific reports – reflected on the Nuclear Regulatory Commission website
  - https://www.nrc.gov/reactors/new-reactors/advanced.html
- US Nuclear Regulatory Commission, including its independent Advisory Committee on Reactor Safeguards, have reviewed and provided input into the approach, and support its endorsement for use

21

21

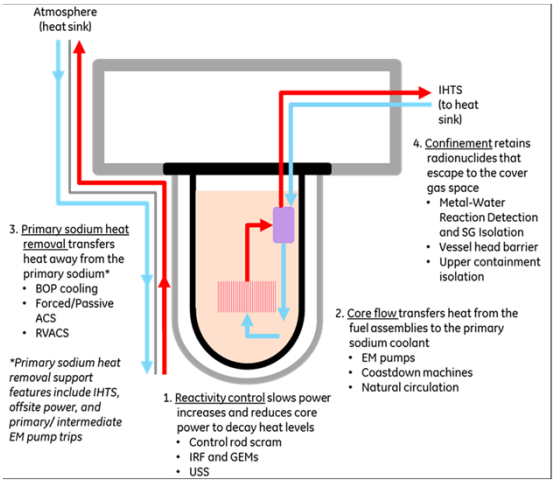
Recent US Experience in Application of the Proposed Approach

LMP Elements Addressed	MHTGR	PBMR	Xe-100	PRISM	Kairos-FHR	MSRE	eVinci	VTR
Preconceptual Design PRA	■	■	■	■	■	■	■	■
Conceptual Design PRA	■	■		■				■
External Hazards PRA	■	■		■				■
Definition of LBEs	■	■	■	■	■	■	■	■
F-C Target Evaluation of LBEs	■	■	■	■	■	■	■	■
Definition of RSFs	■	■	■	■	■	■	■	■
Selection of SR SSCs	■	■	■	■	■	■	■	■
Definition of RFDC	■							■
Definition of SRDCs	■							■
Evaluation of Plant DID				■	■		■	■
Selection of NSRST SSCs				■	■		■	■
Evaluation of Programmatic DID								■

22

22

Pilot Study of PRISM Sodium Fast Reactor (GE-Hitachi)



PRISM PRA Safety Functions

Southern Company

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

PRISM Sodium Fast Reactor
Licensing Modernization Project Demonstration

Project Report
Issued Final

Authors: Thomas Hicks, Matthew Warner, Gary Miller, Jonathan Li

Document Number
SC-29980-201

December 2018

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

Issued final by:

Jan. 29th, 2019

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

Date

23

23

Summary of GE-PRISM Pilot Study Results

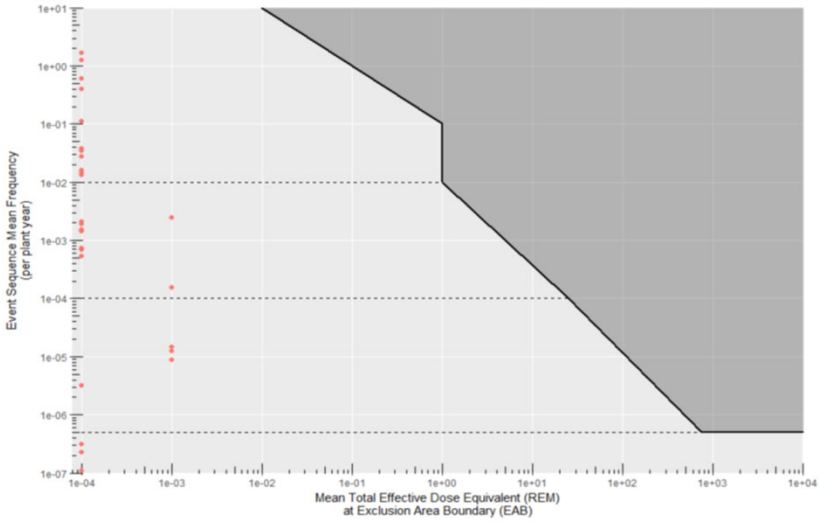
- Each Event Sequence Family (ESF) is assigned to an LBE category based on mean event sequence frequency of occurrence per plant-year summed over all the event sequences in the LBE family
- Applying this criteria to the ESFs of the baseline model, a total of 26 LBEs were identified with categorization breaking down as follows:
  - AOO: 11
  - DBE: 10
  - BDBE: 5

IE Group	Description	AOO	DBE	BDBE
BOP	Balance of Plant Transients	X	X	X
IHTS	Intermediate Heat Transport System			X
IHX	Intermediate Heat Exchanger Leaks	X		
LOF	Loss of Flow	X	X	X
LOOP	Loss of Offsite Power	X	X	
NSSS	Nuclear Steam Supply System Transients	X	X	
SGTR	Steam Generator Tube Rupture		X	X
TOP	Transient Overpower	X	X	

24

24

PRISM LBEs Plotted Against F-C Target



Results of this pilot study reflect large margins between the LBE mean-value points and the target line

25

25

High Level Observations from **PRISM Study**

With the LBEs identified and categorized, there is now a manageable set of events to analyze that represent a much larger population of PRA event sequences. The grouping process in terms of event counts is summarized below.

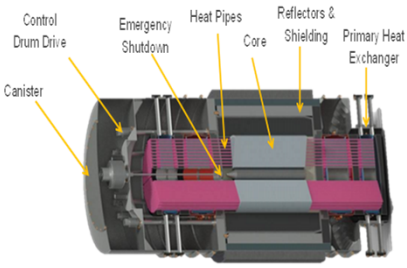
Observations were that utilizing this approach results in:

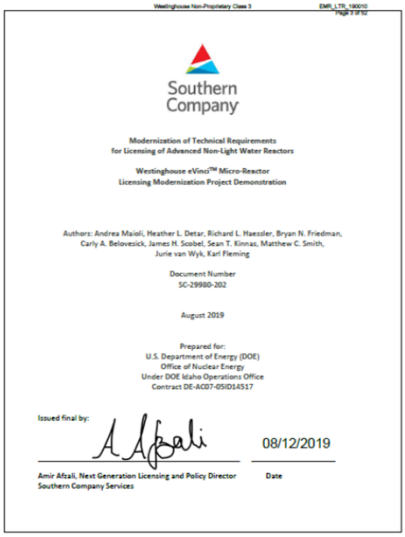
- A systematic, practical, and reproducible framework for selection of LBEs
- Better communication of PRA to designers
- Identification of other design approach options

26

26

Pilot Study of eVinci Micro-Reactor (Westinghouse)





Southern Company

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

Westinghouse eVinci™ Micro-Reactor Licensing Modernization Project Demonstration

Authors: Andrea Maioli, Heather L. Detar, Richard L. Haessler, Bryan N. Friedman, Carly A. Belovesick, James H. Scobel, Sean T. Kinnas, Matthew C. Smith, Jurie van Wyk, Karl Fleming

Document Number SC-29980-202

August 2019

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

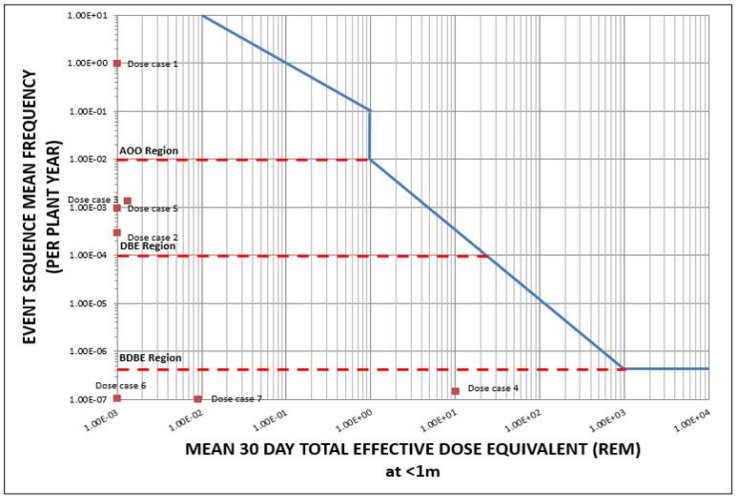
Issued final by: 08/12/2019

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

27

27

eVinci LBE Evaluation Against F-C Target



28

28

Establishing Required Safety Functions

29

29

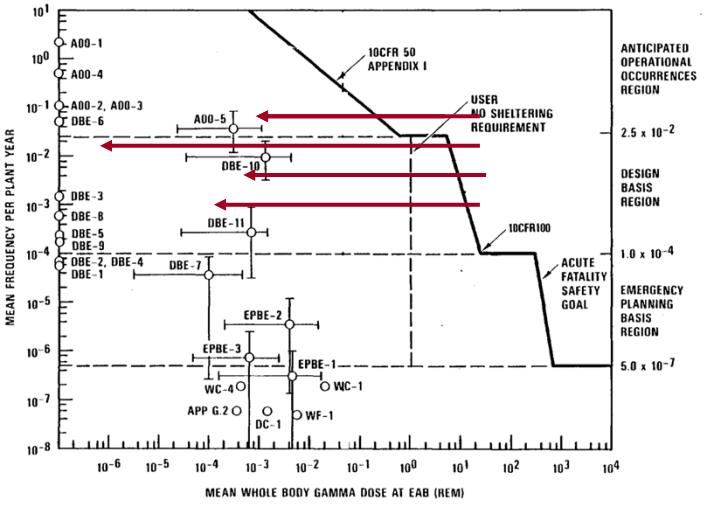
Identification of Required Safety Functions (RSFs)

- Required Safety Functions (RSFs) are derived from the Fundamental Safety Functions
- RSFs are those functions that:
  - if not fulfilled would lead to increase in DBE consequences beyond the F-C target;
  - or would increase the frequency of high consequence BDBEs beyond the F-C target
- RSFs also serve to define capabilities and functions that must be preserved to deliver the safety case
- SSCs that are available to perform the RSFs may include:
  - Inherent or intrinsic reactor features
  - Passive SSCs
  - Active SSCs
  - Combinations of the above
- Advanced reactor designs typically include multiple means of achieving each RSF.

30

30

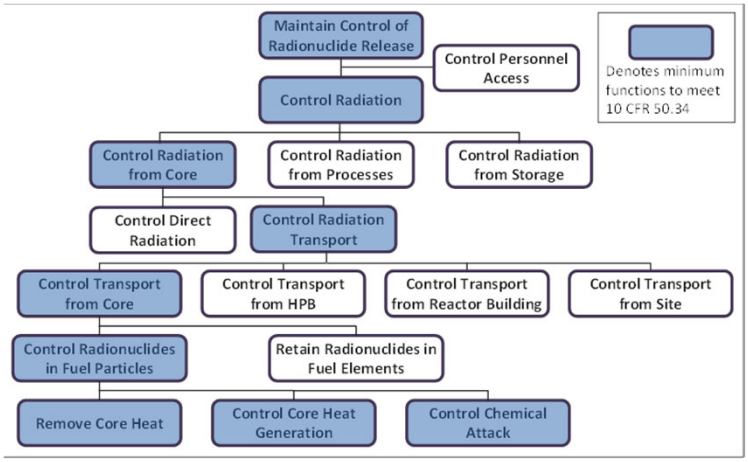
MHTGR Example for Identifying RSFs



31

31

MHTGR Required Safety Functions



32

32

Classification of Structures, Systems & Components (SSCs)

33

33

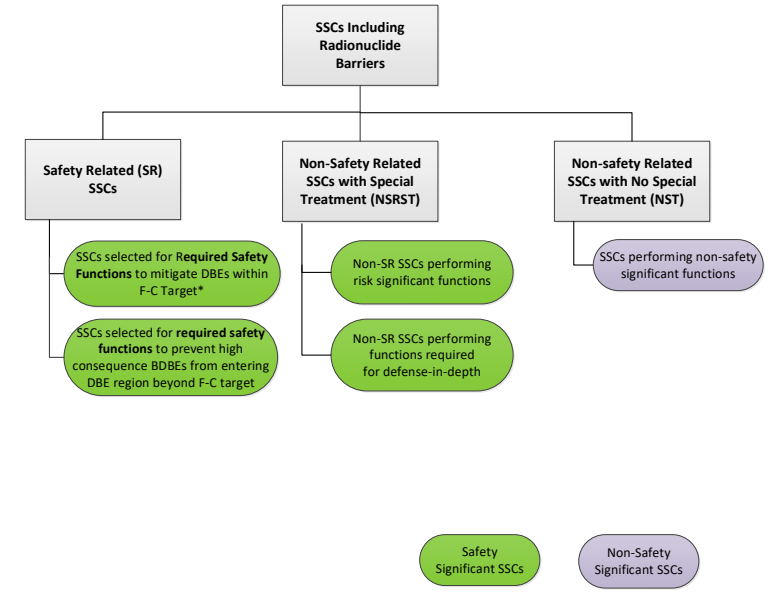
SSC Safety Categories

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

34

34

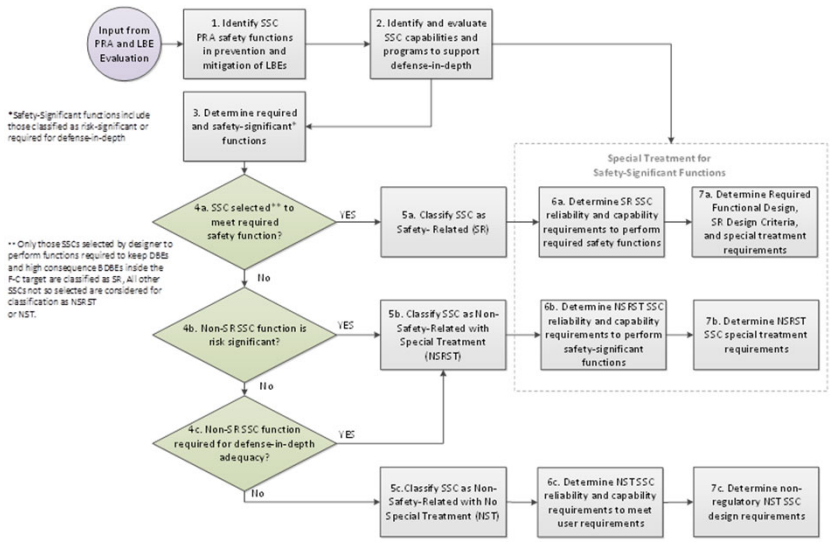
SSC Safety Categories



35

35

SSC Safety Classification Approach



36

36

SSC Risk Significance

- **A prevention or mitigation function of the SSC is necessary to meet the design objective of keeping all LBEs within the F-C target.**
  - The LBE is considered within the F-C target when a point defined by the upper 95%-tile uncertainty of the LBE frequency and dose estimates are within the F-C target.
- **The SSC makes a significant contribution to one of the cumulative risk metrics used for evaluating the risk significance of LBEs.**
  - A significant contribution to each cumulative risk metric limit is satisfied when total frequency of all LBEs with failure of the SSC exceeds 1% of the cumulative risk metric limit. The cumulative risk metrics and limits include:
    - The total frequency of exceeding of a site boundary dose of 100 mrem <1/plant-year (10 CFR 20)
    - The average individual risk of early fatality within 1 mile of the Exclusion Area Boundary (EAB) < 5×10^{-7}/ plant-year (QHO)
    - The average individual risk of latent cancer fatalities within 10 miles of the EAB shall not exceed 2×10^{-6}/plant-year (QHO)

37

37

Derivation of Special Treatment Requirements

- **SR SSCs**
  - Required Functional Design Criteria (RFDC) derived from Required Safety Functions (RSFs); may be used in formulating principal design criteria
  - Component level Safety Related Design Criteria (SRDC) developed from RSFs
- **SR and NSRST SSCs**
  - SSC reliability and capability performance targets
  - Focus on prevention and mitigation functions identified in LBEs
  - Integrated decision-making process to derive additional specific special treatment requirements, if any
  - Reflects concepts from existing reactors from a “forward fit” perspective
  - Reflects a risk-informed and performance based structure

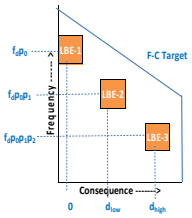
38

38

Roles of SSC Reliability and Capability in Prevention and Mitigation of Accidents

Plant Distrubance	Plant features prevent Inititating event?	SSC_1 Prevents Fuel Damage?	SSC_2 Limits Release?	LBE	End State	Defense-in-Depth Layers Challenged [1]	Frequency	Dose
f_d	Yes			N/A	Disturbance controlled with no plant trip	Layer 1	f_d	0
	p_0 No	Yes		1	No fuel damage or release	Layer 2	$f_d p_0$	0
		p_1 No	Yes	2	Fuel damage w/ limited release	Layer 3	$f_d p_0 p_1$	d_{low}
			p_2 No	3	Fuel Damage w/ un-mitigated release	Layers 4 and 5	$f_d p_0 p_1 p_2$	d_{high}

[1] See Figure 2-4 for definition of defense-in-depth layers



SSC	LBEs	Function	SSC Performance Attribute for Special Treatment
Plant	N/A	Prevent initiating event	Reliability of plant features preventing initiating event
SSC_1	1	Mitigate initiating event	Capability to prevent fuel damage
	2	Prevent fuel damage	Reliability of mitigation function
	3	Help prevent large release	Reliability of mitigation function
SSC_2	2	Mitigate fuel damage	Capability to limit release from fuel damage
	3	Prevent unmitigated release	Reliability of mitigation function

39

39

SSC Classification Summary

- Describes safety categories of SR, NSRST, and NST
- SR and NSRST SSCs classified as safety significant
- Absolute risk metrics used to determine SSC and LBE risk significance
- NSRST SSCs include other risk significant SSCs and SSCs requiring some special treatment for DID adequacy
- Minimum special treatment is the formulation of reliability and capability targets for safety significant SSCs and a program to monitor performance against targets
- Reliability and capability targets linked to the prevention and mitigation functions of the safety significant SSCs, respectively
- Quality Assurance programs are focused on performance of SR SSCs in the performance of the RSFs
- Owners quality programs applied to NSRST SSCs in the performance of their prevention and mitigation functions responsible for classification as NSRST

40

40

Deriving DBAs from DBEs

41

41

Deriving DBAs from DBEs

- Each identified DBE has a corresponding DBA
- DBAs are used to set design criteria and performance objectives for the design of safety-related SSCs.
- In this approach, DBAs are derived from the risk-informed DBEs.
- Within this DBA category, it is assumed that the required functions needed to address safety challenges represented in a DBE are performed exclusively by safety-related SSCs, and that all non-safety-related SSCs that perform these same functions are assumed to be unavailable.
- When this approach is applied, the expected frequency of occurrence for a DBA is typically lower than the expected DEC frequency

42

42

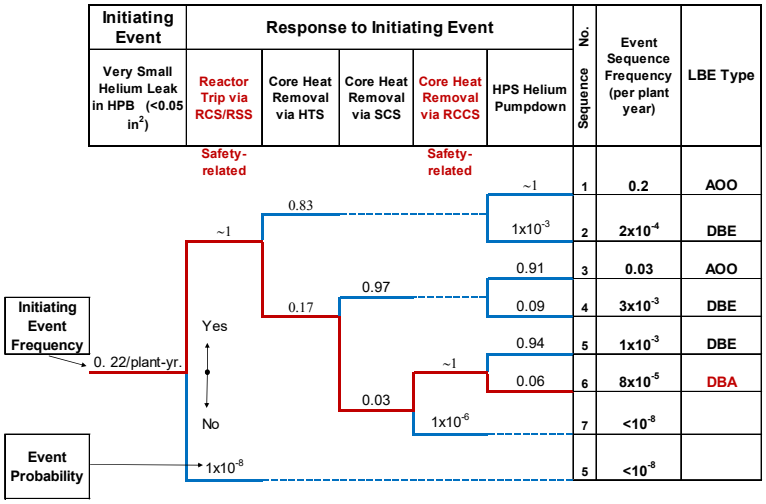
Example DBEs and DBAs from General Atomics Modular HTGR Design – Provide Cooling Function With Helium Leaks

DBE	Design Basis Events	DBA	Design Basis Accidents
DBE-10	Moderate HPB leak with successful reactor trip, continued forced cooling, release of circulating activity and lift-off of plateout to reactor building involving a single reactor module. (corresponds to PRA sequence family with frequency of $1x10^{-2}$/plant-year or about $3x10^{-3}$/reactor-year)	DBA-10	Moderate HPB leak with successful reactor trip, failure of forced cooling via Main loops and SCS, passive cooling via RCCS, release of circulating activity, delayed fuel release, and lift-off of plateout to reactor building involving a single reactor module. (corresponds to PRA sequence family with frequency of $6x10^{-8}$/plant-year or about $1.5x10^{-8}$/reactor-year)
DBE-11	Small HPB leak with successful reactor trip, failure of forced cooling via Main and SCS Loops, passive cooling via RCCS, partial release of circulating activity and delayed fuel release to reactor building involving a single reactor module. (corresponds to PRA sequence family with frequency of $3x10^{-4}$/plant-year or about $8x10^{-5}$/reactor-year)	DBA-11	Small HPB leak with successful reactor trip, failure of forced cooling via Main and SCS, partial release of circulating activity and delayed fuel release to reactor building involving a single reactor-module. (corresponds to PRA sequence family with frequency of $<10^{-8}$/plant-year or $<10^{-8}$/reactor-year)

43

43

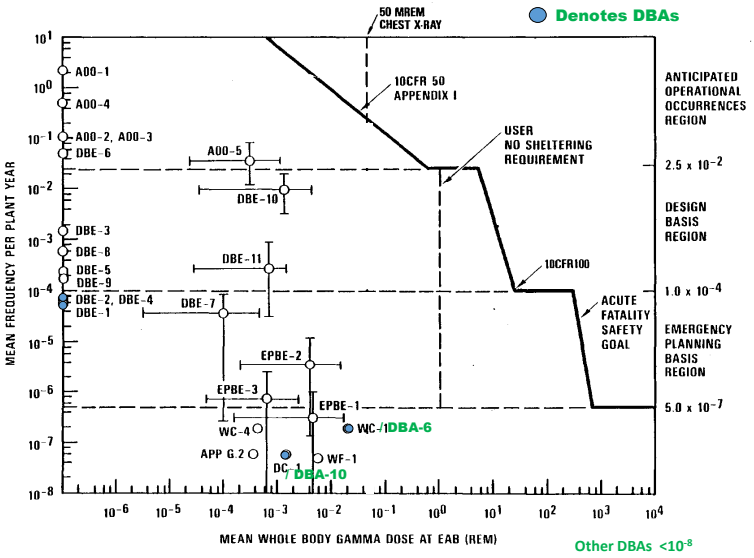
DBAs Rely Only on Safety-Related SSCs (DBA-11 example)



44

44

MHTGR DBEs, DBAs, and BDBEs (aka EPBEs) on F-C Plot (circa 1987)



45

45

Defense in Depth Evaluation

46

46

Evaluating Defense in Depth (DID) Adequacy General Objectives

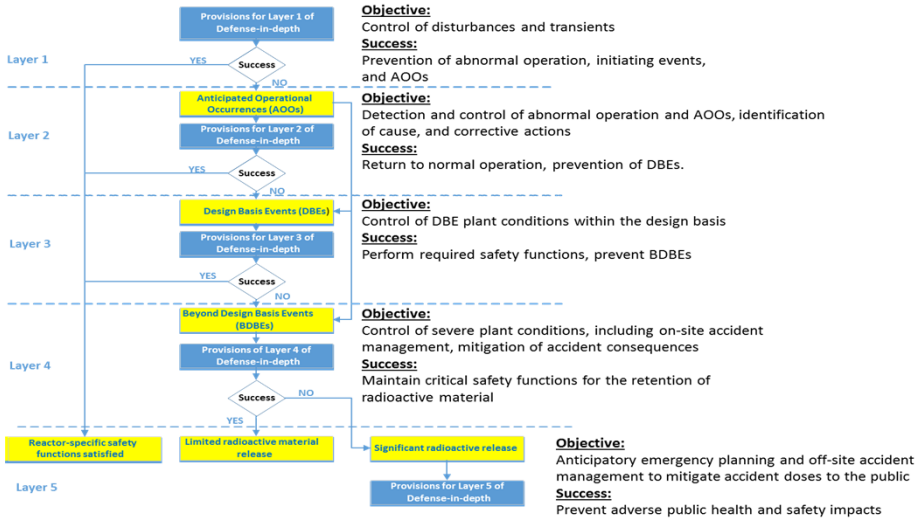
General objectives of proposed approach for evaluating DID adequacy:

- Systematic and Reproducible
- Sufficiently Complete
- Available for Timely Input to Design Decisions
- Risk-Informed and Performance-Based
- Reactor Technology-Inclusive
- Compatible with Applicable Regulatory Requirements

47

47

Layers of Defense Adapted from IAEA (Adapted to address multiple reactors on a site and to avoid LWR-centric terms)



48

48

DID Adequacy Evaluation Process

- DID baseline evaluation is developed using an Integrated Decision Process (IDP) and updated during each design/licensing phase

- Defense-in-depth is deemed as adequate when:
  - Plant capability DID is deemed to be adequate.
  - Plant capability DID guidelines are satisfied.
  - Review of LBEs is completed with satisfactory results
  - Programmatic DID is deemed to be adequate.
  - Performance targets for SSC reliability and capability are established
  - Sources of uncertainty in selection and evaluation of LBE risks are identified.
  - Special treatment for all SR and NSRST SSCs is sufficient

DID Adequacy Evaluation

Plant Capability Defense-In-Depth Attributes

The table below provides a listing of the integrated DID attributes and principal evaluation focus of the Plant Capability DID evaluation scope using an IDP

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

DID Adequacy Evaluation (cont.)

Plant capability DID is deemed to be adequate when:

- Plant capability DID guidelines in adequacy table (next slide) are satisfied
- Risk margins against F-C target are sufficient
- Risk margins against Cumulative Risk Targets are met
- Role of SSCs in the prevention and mitigation at each layer of defense challenged by each LBE is understood
- Prevention/mitigation balance is provided across layers of defense
- Classification of SSCs into SR, NSRST, and NST is appropriate
- Risk significance classification of LBEs and SSCs are appropriate
- Independence among design features at each layer of defense is sufficient
- Design margins in plant capabilities are adequate to address uncertainties identified in the PRA

51

51

DID Adequacy Evaluation (cont.)

Guidelines for Establishing the Adequacy of Overall Plant Capability Defense-in-Depth

[Any SSCs necessary to meet this guideline would be regarded as performing a safety function necessary for adequacy of plant capability DID]

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

Notes:

[a] The plant design and operational features and protective strategies employed to support each layer should be functionally independent

[b] Non-regulatory user requirements for plant reliability and availability and design targets for transient cycles should limit the frequency of initiating events and transients and thereby contribute to the protective strategies for this layer of DID. Quantitative and qualitative targets for these parameters are design specific.

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

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

52

52

DID Adequacy Evaluation (cont.)

- A key element of the risk-informed, performance-based evaluation of DID is a systematic review of the LBEs against the layers of defense
- LBE evaluations focus on the following questions:
  - Is the selection of initiating events and event sequences reflected in the LBEs sufficiently complete?
  - Are the uncertainties in the estimation of LBE frequency, plant response to events, mechanistic source terms, and dose well characterized?
  - Are there sources of uncertainty not adequately addressed?
  - Have all risk significant LBEs and SSCs been identified?
  - Has the PRA evaluation provided an adequate assessment of "cliff edge effects?"
  - Is the technical basis for identifying the required safety functions adequate?

53

53

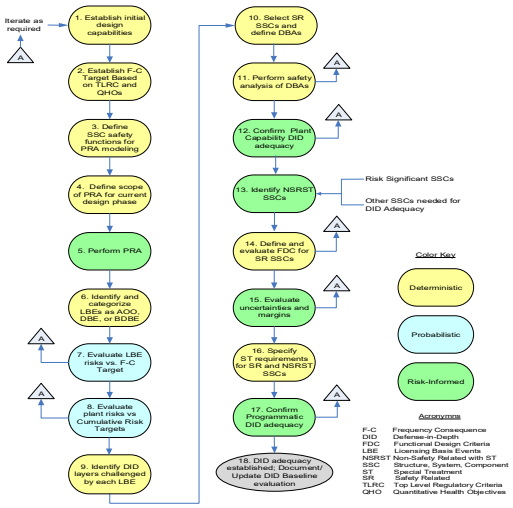
Wrap-up and Summary

54

54

Integrated View of Approach Tasks

- Tasks are iterative; not sequential
- Tasks can begin early in the conceptual design process and mature with the design evolution
- Discovery mode or confirmatory mode
- Event sequence families from a PRA used as key input to selecting LBEs
- SSC classification and evaluation are integrated with the LBE selection and evaluation tasks
- Defense-in-depth evaluation is integrated with the LBE selection and evaluation and is an integral part of the SSC classification and performance requirement determination
- Tasks include deterministic and probabilistic elements and involve RIPB decisions to support the design and formulate and evaluate the safety case.



55

55

Observations

- The proposed approach addresses these overarching goals :
  - **Risk-informed:** A complementary approach that combines both deterministic and probabilistic information into the decision-making process
  - **Understandable, traceable, and reproducible**: The criteria and guidance developed as part of this approach should have a clearly stated basis, and each step of the process should be identified and clearly described
  - **Defensible**: Whenever possible, known technology should be used to develop the technical basis
  - **Flexible**: New information, knowledge, research results etc., should be incorporated, in an efficient and effective manner,
  - **Performance-based**: The safety approach, technical bases, and safety requirements should be goal setting and performance based
- US pilot studies have confirmed these characteristics are being achieved

56

56

Next Steps & Proposed Timeline

- Dec 2019: Based on feedback and inputs from meeting this week, transmit draft paper to GIF-RSWG summarizing the approach
- April 2020: Address/resolve GIF-RSWG inputs (RSWG meeting?)
- May 2020: Transmit updated and near-final draft report to GIF-RSWG and WGSAR for review/comment
- Oct 2020: Discuss and finalize report at coordinated GIF-RSWG and WGSAR meetings

57

57