U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Licensing Review Framework for Advanced Reactors Instrumentation and Controls (I&C)

Workshop 2

April 4, 2023

Advanced Reactor Program

Introduction and Requests for Workshops on I&C Licensing Framework for Advanced Reactors

- Final I&C Design Review Guide (DRG) issued in February 2021 (ML21011A140) for I&C design reviews by NRC staff
- NRC staff reviews / pre-application engagements underway for a variety of potential LWR and non-LWR I&C designs
- NRC staff engaged by industry interested in the background and details on the DRG—and relationship to NEI documents
- No regulatory decisions will be made in these workshops

Workshop 2 Agenda

- Overview of Workshop 1 and Follow-up Questions on Non-Safety-Related Special Treatment (NSRST) Structure, System, and Component (SSC) Classification
- Discussion of Alternate Frameworks
- NRC Staff Perspectives on Design Basis Accident (DBA) Analysis Described in the Licensing Modernization Project (LMP)

Workshop #2

Advanced Reactor Digital I&C Licensing

April 4, 2023

NUCLEAR ENERGY INSTITUTE

Follow-Up Question – Non-Safety-Related Special Treatment (NSRST)

Question 1: How does the NSRST categorization compare to previously used categorizations such as Regulatory Treatment of Non-Safety Systems (RTNSS) and Risk-Informed Safety Class 2 (RISC-2) which also describe supplemental requirements for non-safety-related SSCs that perform safety significant functions?

Alternate Frameworks

General Atomics Electromagnetic Systems

An Introduction to the Functional Safety:

Application of Functional Safety (Risk-Informed Performance-Based Approach) in Advanced Nuclear Reactor ARC-20 FMR

02/23/2023

Presented to: NRC/NEI DI&C Industry Working Group

Prepared By:

Mohammad Alavi, P.E., FS Eng (TÜV Rheinland)

Nuclear I&C and Functional Safety Lead

Nuclear Reactor Design and Analysis

GA-EMS NTM Division

Agenda

- Generic Introduction to Functional Safety
- Application of Functional Safety (RIPB Approach) in Nuclear
- Example of Functional Safety Implementation in General Atomics ARC-20 FMR

Introduction

- **What is Functional Safety?**

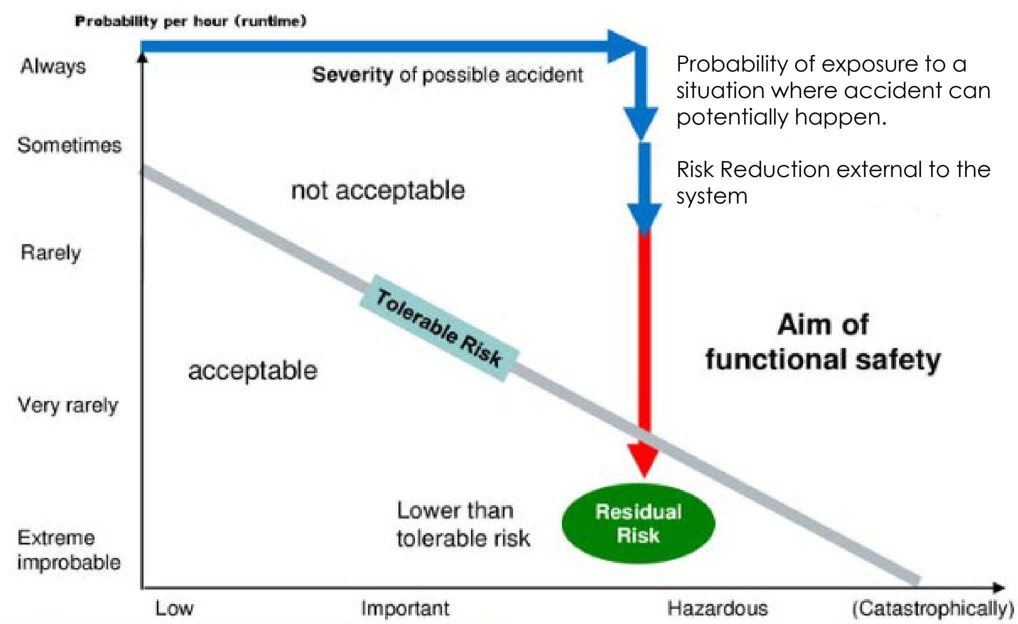
Definition of Safety: Freedom from unacceptable risk of physical injury or of damage to the health of people, either directly or indirectly as a result of damage to property or to the environment.

Functional Safety: FS is part of the overall safety of a system or piece of equipment that looks at the aspects of safety that relates to the function of a device or system and depends on automatic protection operating correctly and predictably in response to its inputs or failures.

In other word, Functional Safety is, "Systems that lead to the freedom from unacceptable risk of physical injury or damage to the health of people either directly or indirectly by the proper implementation of one or more automatic protection functions (often called safety functions). The automatic protection system must be able to properly handle likely human errors, systematic errors, hardware/software failures and operational/environmental stress.

Risk Reduction and Graded Approach

- **Functional Safety is a risk-informed and performance-based approach to address safety with implementation of automated protection functions. Probabilistic methods are used in assessment, design, and evaluation.**



- **Risk Evaluation and Functional Safety**

When it comes to the risk evaluation, functional safety is all about risk reduction to a level lower than tolerable risk.

So, risk assessment and hazard analysis is an essential part of functional safety life cycle.

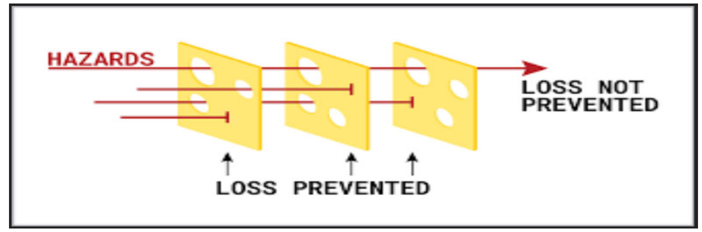
Functional Safety views on risks:

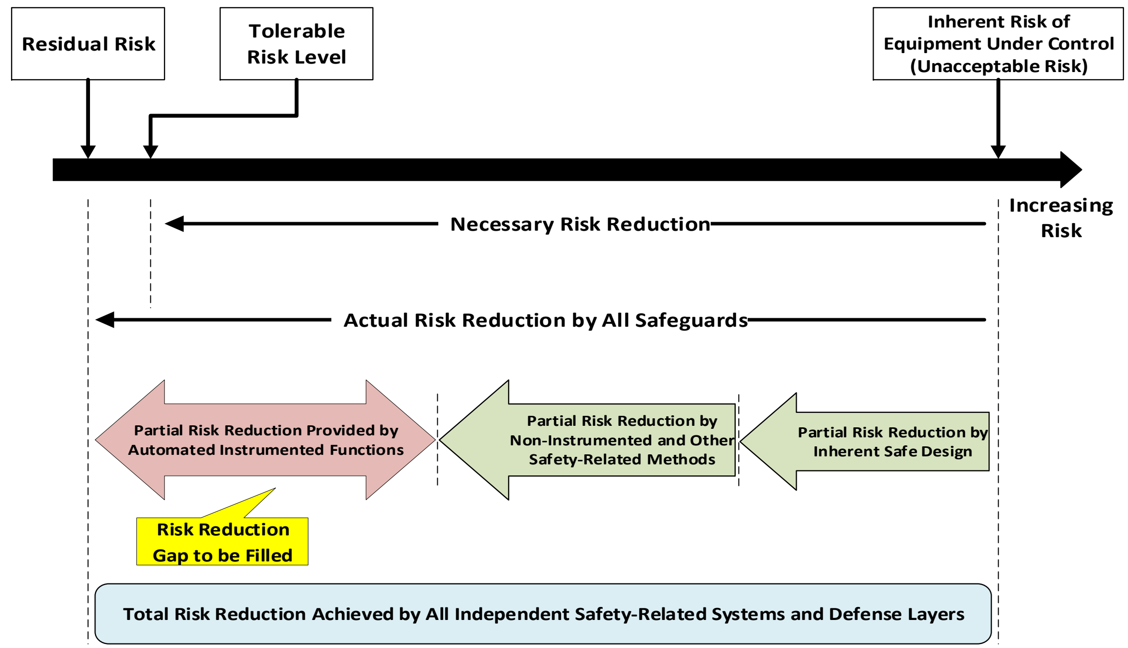
- Zero risk can never be reached, only probabilities can be reduced
- Non-tolerable risks must be reduced (ALARA*)
- Optimal, cost-effective safety is achieved when addressed in the entire safety lifecycle

** ALARA: As Low As Reasonably Achievable*

Tolerable Risk Level

- **How to Achieve to Tolerable Risk Level**
  - No defense layer is fault free no matter how high its reliability is.
  - Credible and independent layers of protection are needed to overcome random failures, systematic failures, human errors, and common cause failures.
  - Protection layers reduce the probability of incident, and/or reduce the severity of possible incident.
  - Reliability of each protection layer is determined by probabilistic methods.





GENERAL ATOMICS ELECTROMAGNETICS

Attributes of Risk Reduction Layers

- Defense layers must have at least four key characteristics (S A I D) to be eligible and credible as a protection layer:
  - **Specific**
    Protection layer must be designed solely to prevent or mitigate the consequences of one potentially hazardous event. Multiple causes may lead to the same hazardous event. The action of one protection layer is necessary.
  - **Auditable**
    Protection layer must be designed in a way that to permit validation of function and probability of failure on demand (PFD), including drill for human error and systematic failure, in a regular periodic manner. This is the ability to inspect information, documents, procedures, etc. to demonstrate the adequacy of protection and adherence to the requirements.
  - **Independent**
    The performance of protection layer should not be degraded or affected by the initiating cause of failure nor is it influenced by the failure of other protection layers. This is mainly for common cause failures.
  - **Dependable and Reliable**
    This is the probability that the protection layer will operate accurately toward the intended event under stated conditions for a specific time period. The protection layer must be dependable and have a reliability higher than reliability target for preventing or mitigating the hazard scenario.

Regulatory Framework

- **Major Regulations and Codes Governing Functional Safety**

10CFR50, 10CFR52 – Nuclear Regulatory Commission
29CFR1910 – OSHA Process Safety Management
RG1.233 – Risk-Informed Performance-Based Methodology for Non-LWR
NUREG/KM-0009 – Observation of Defense-in-Depth
NRC DRG – I&C for Non-Light-Water Reactors (TBD)
NEI 18-04 – Risk-Informed Performance-Based Guide for AR
DOE-STD-1189 – Integration of Safety into Design Process
DOE-STD-1195 – Safety Instrumented Systems
DOE-STD-3009 – Safety Analysis
DOE-STD-1628 – PRA for Nuclear Safety Applications
IAEA SSR-2/1 – Safety of Nuclear Power Plants
MIL-STD-882E – System Safety

GENERAL ATOMICS ELECTROMAGNETICS

Principles of Functional Safety

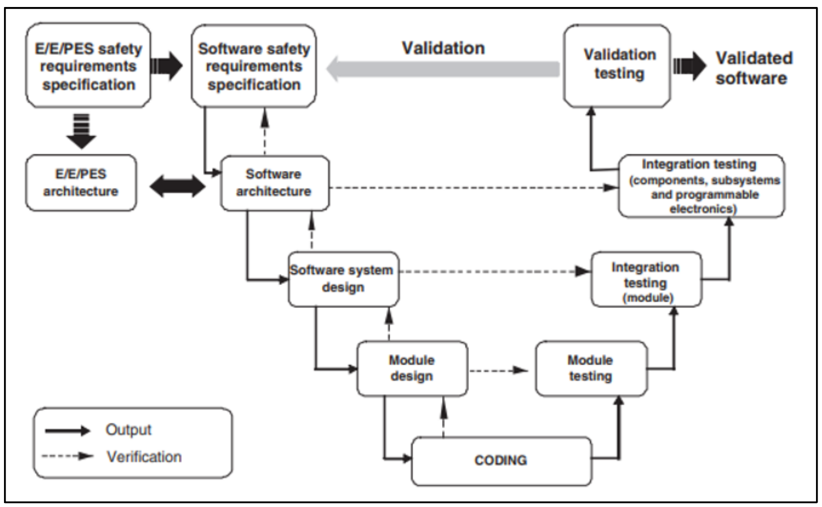
- There are two fundamental principles:
  - An engineering process called the **Safety Lifecycle** is defined to discover and eliminate design errors and omissions.
  - A probabilistic failure approach to account for the safety impact of device failures.

- The safety life cycle are divided and grouped into three categories:
  - Phases to address analysis
  - Phases to address realization
  - Phases to address operation

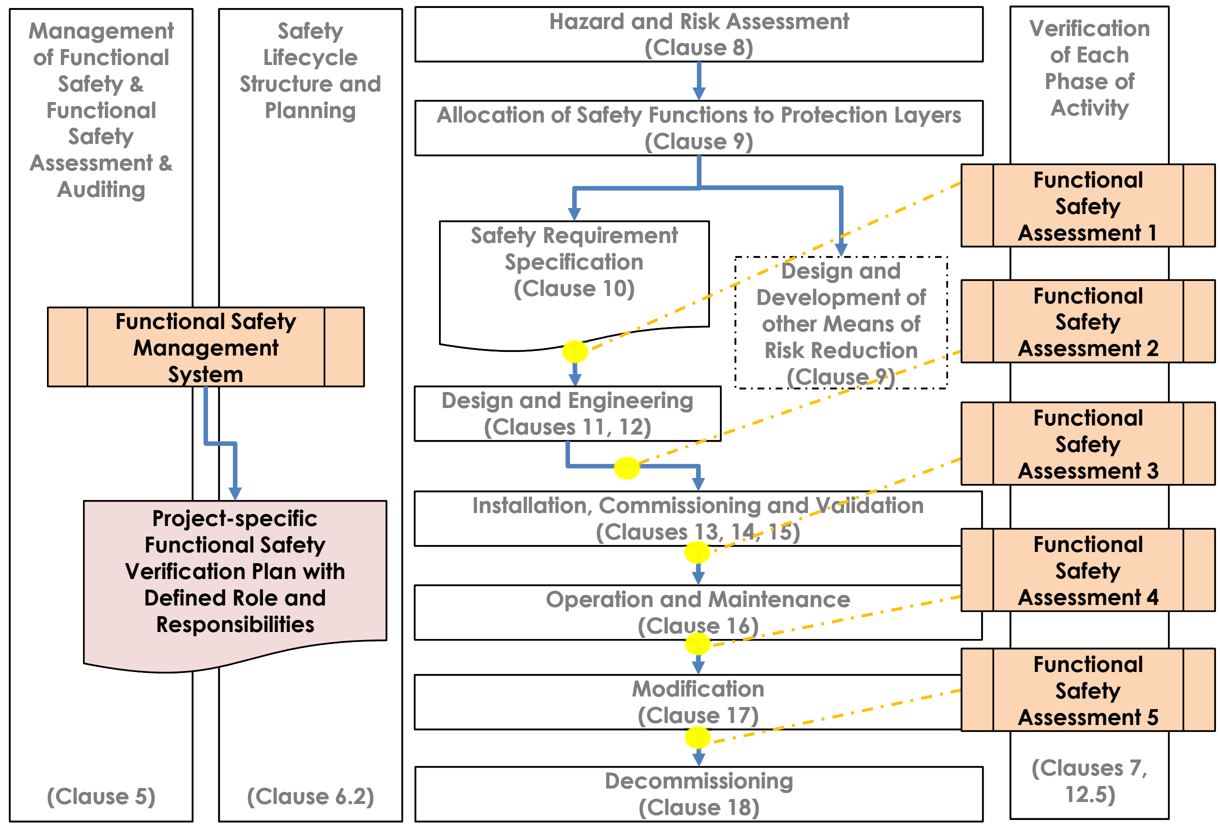
- Concepts of probabilistic risk for each safety function:
  - The risk is a function of frequency (or likelihood) and consequence severity of each hazardous event.
  - The risk is reduced to a tolerable level by applying protection functions.

Safety Life Cycle

- Safety Lifecycle:
  - Overall Process and Functional Safety Management
  - Hardware Architecture and Design
  - Software Development Lifecycle



Software Systematic Development Lifecycle (V-Model) (ref. IEC 61508)

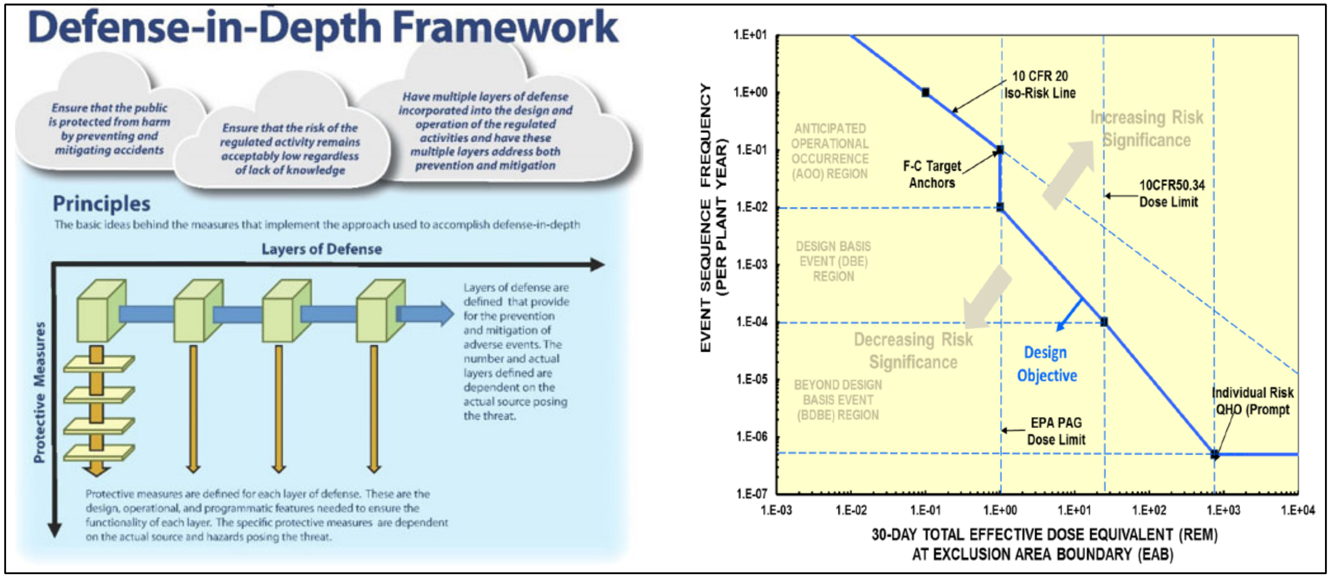


Overall Safety Lifecycle (ref. IEC 61508, 61511)

GENERAL ATOMICS ELECTROMAGNETICS

Nuclear Application

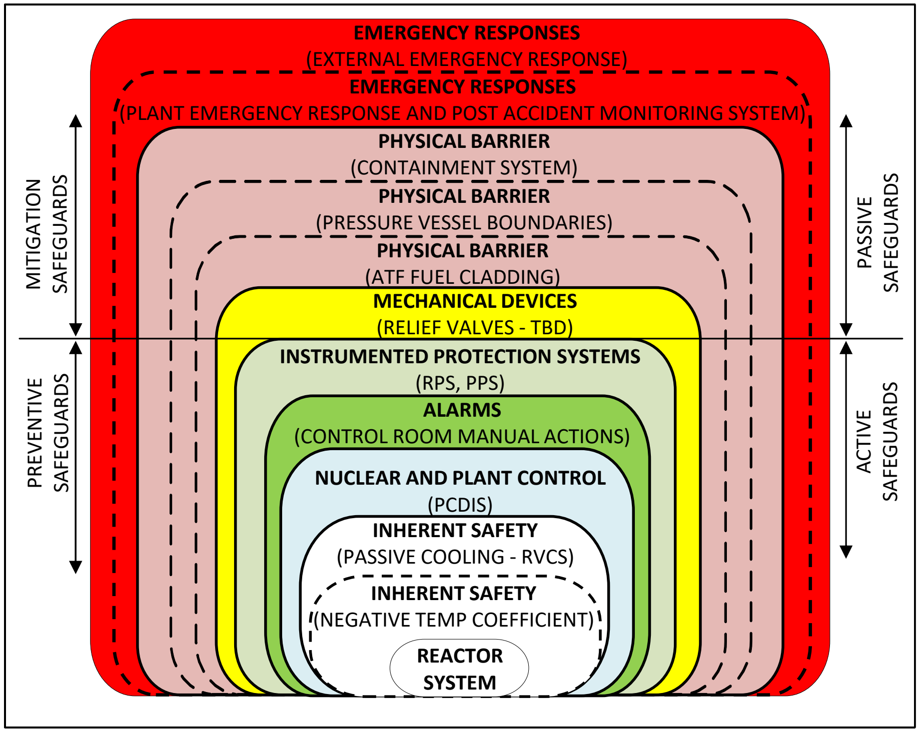
- Nuclear Reference
  - NUREG/KM-0009, NEI 18-04
- F-C Target
  - Decreasing risk significance to a margin below F-C curve
- Defense-in-Depth Framework
  - Multiple layers of defense
  - Independent layers of defense
  - Physical and functional independence
  - Separation from initiating cause of incident
  - Number of defendant layers based on the level of hazard and F-C target
  - Layer of defense to provide prevention and mitigation



- Protective measures for each layer of defense to ensure its functionality and reliability (examples):
  - Design, operational, and programmatic features
  - Redundancy, and diversity considerations
  - Address common cause failure
  - Fail safe design
  - Single point of failure vulnerability criterion, etc.

ARC-20 FMR Layer of Defense Model

- 1st Group – Inherent Safety into Design:
  - Negative Reactivity Temperature Coefficient
  - Passive Cooling System (RVCS)
- 2nd Group – Automated Systems:
  - Nuclear and Plant Control (PCDIS)
  - Alarm System (Control Room and Operator Actions, PMS)
  - Instrumented Protection Systems (RPS, PPS)
- 3rd Group – Mechanical Devices
  - Relief Valves (TBD)
- 4th Group – Physical Barriers
  - ATF Cladding
  - Vessel and Pressure Boundaries
  - Containment System
- 5th Group – Mitigation and Emergency Response
  - Post Accident Monitoring System (PAMS)
  - Emergency Response



*Defense-in-Depth Framework (Independent Layers of Defense**)*

*** Only those defense layers can be credited for risk reduction that are independent from initiation cause of incident and other defense layers for that specific hazard scenario.*

BACK-UP SLIDES

Introduction

- **Why Is Functional Safety Important?**

Complex technology is an integral part of our life, and day to day activities as well as industries. The all-encompassing objective of functional safety is to prevent risk to human lives caused either directly or indirectly from the operation of these systems. This includes preventing risk caused by damage to equipment, property, or the environment.

Functional safety is becoming more important as the types of controls and hardware being used are increasingly more complex. Software is also increasingly used in safety-critical applications and industrial plants including nuclear. Thus, these complex hardware and software need to be safe, secure, and reliable.

The critical factor at play is the appropriate and correct implementation of protection functions known as safety functions.

Functional Safety Scope

- **What Is Scope of Functional Safety**

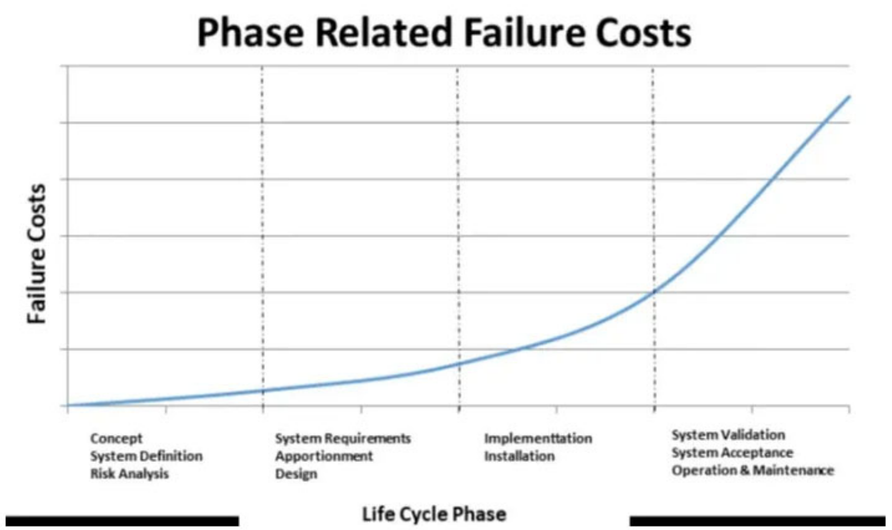
The scope of functional safety is end-to-end, in that it must treat any function of a component or subsystem as part of the operation of the entire system's automatic protection function. Thus, although the standards for functional safety are generally focus on electrical, electronics (hardware and software), and programmable systems, in practice functional safety methods must extend to the nonelectrical, nonelectronic, and non-programmable components of the entire system.

Functional Safety is a risk-informed and performance-based approach to address safety and implement the automated protection functions. Probabilistic methods are used in assessment, design, and evaluation.

GENERAL ATOMICS ELECTROMAGNETICS

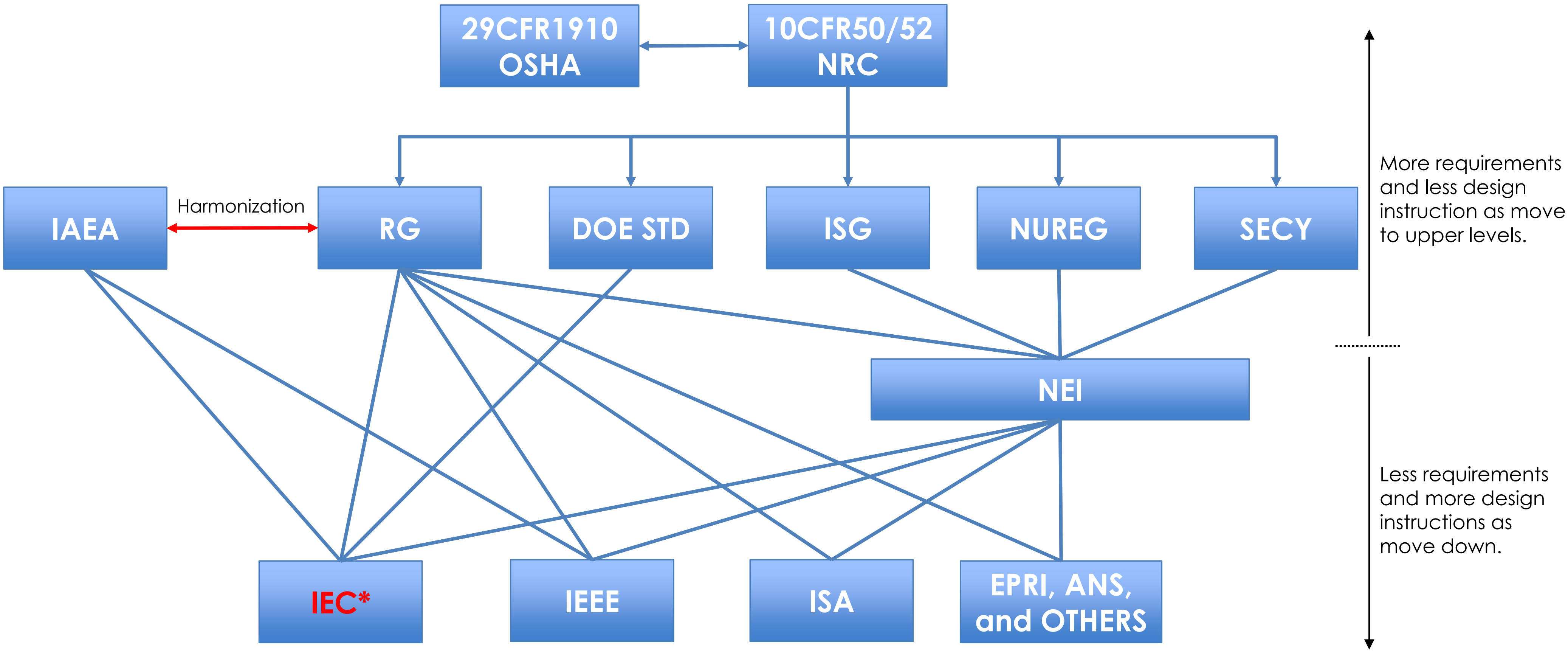
When to Implement

- **When to Implement Functional Safety Plan**
  It is best practice to plan and implement functional safety very early in design stages. This will allow the design teams to develop robust plans that include functional safety milestones - catching any failings as they occur in real-time will save time and money instead of retroactively addressing issues.



GENERAL ATOMICS ELECTROMAGNETICS

Regulatory Framework and Industry Standards



GENERAL ATOMICS ELECTROMAGNETICS

IEC 61508 - Global Industry Standard

- IEC 61508 is a basic functional safety standard as a global standard applicable to all industries.
- The concept and framework is flow down to a lower-level standards specific to each industry.

- System safety principles underpinning functional safety were initially developed in the military, nuclear and aerospace industries, and then taken up by rail transport, process and control industries developing sector specific standards.

- History of evolving functional safety concept:

1969	1980	1996	1998
MIL-STD-882 **Military**	**IEEE 603** **Nuclear**	**ISA 84** **Process**	**IEC 61508** **Global for all** **Automated Protection Systems**

Military Aerospace
- **MIL-STD-882** – System Safety

Aviation
- **DO-178** – Software
- **DO-254** – Hardware

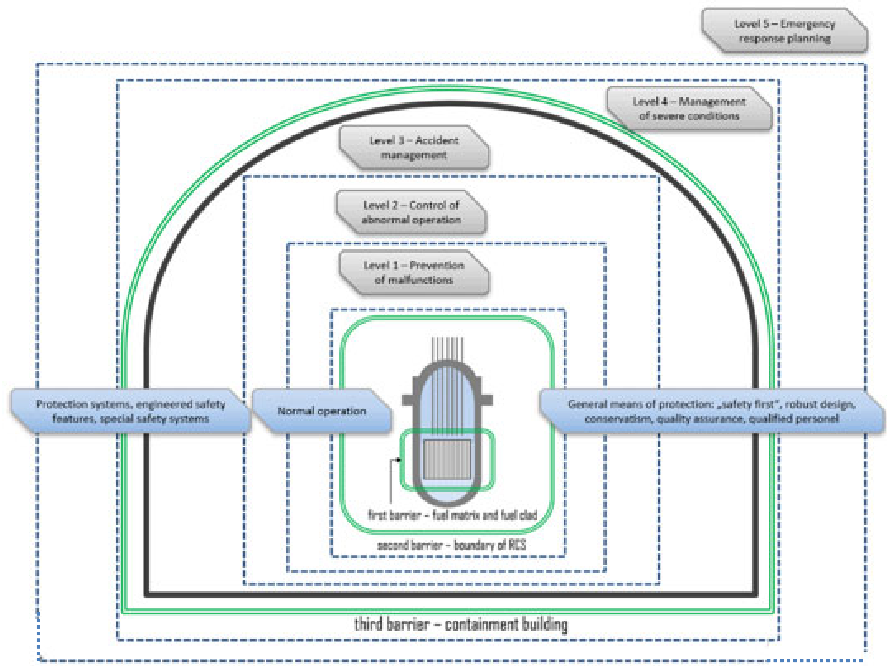
GENERAL ATOMICS ELECTROMAGNETICS

Principles of Functional Safety

- Functional safety standards are applied across all industry sectors dealing with safety critical requirements and are especially applicable anytime software commands and/or E/EE/PES controls or monitors a safety function.
- Functional safety standards consisting of methods on how to apply, design, deploy and maintain automatic protection systems called safety-related systems.
- The Functional safety focus is on ensuring safety critical functions and functional threads in the system, subsystem and software are analyzed and verified for correct behavior per safety requirements, including functional failure conditions, faults, and appropriate mitigation in the design.
- Functional safety is becoming the normal focused approach on complex software intensive systems and highly integrated systems with safety consequences.
- The fundamental concept is that any safety-related system must work correctly or fail in a predictable (safe) way.

Nuclear Application (ARC-20 FMR)

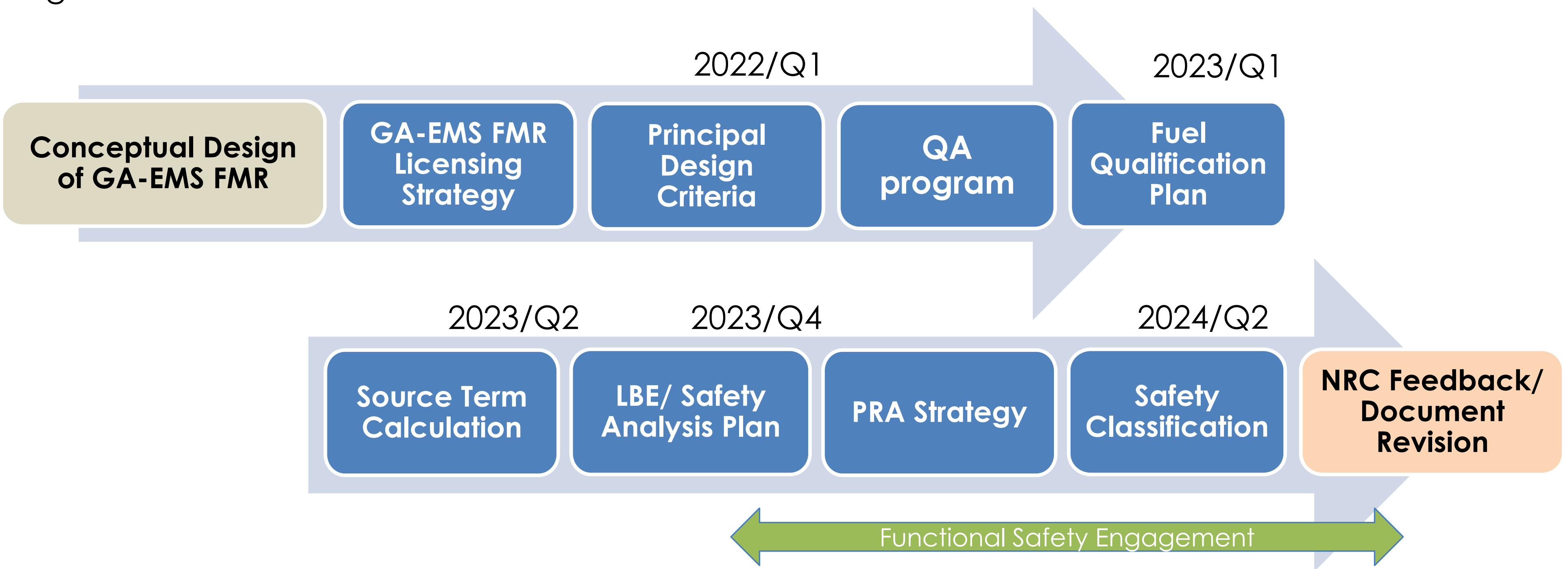
- Nuclear Safety Defense-in-Depth Principle
  - Combination of physical barriers and functional barriers
  - Active safeguards for prevention
  - Passive safeguards for mitigation
  - Instrumented and non-instrumented layers
  - Five groups of independent layers of defense
- Automated Layers of Defense:
  - Nuclear plant control
  - Alarm systems and operator actions
  - Instrumented protection systems
- Non-Instrumented Layers of Defense
  - Inherent safe design, and passive cooling system
  - Physical barriers



GENERAL ATOMICS ELECTROMAGNETICS

FMR Pre-Application Regulatory Engagement Plan

- Digital I&C licensing pre-application is not specifically planned as part of FMR phase 1 activities; however, DI&C and functional safety engagement with overall FMR pre-application process will begin mid 2023.



Reference: C. Fu, H. Choi, and J. Bolin, "The Fast Modular Reactor (FMR) Pre-application Regulatory Engagement Plan," *Tran. Am. Nucl. Soc.* **125**, 794–796 (2021 ANS Winter Meeting).

NRC Advanced Reactor Digital Instrumentation and Control Workshop

February 23, 2023

BWRX-300 Topics for Discussion

Licensing Modernization Process

NEI 18-04
Risk-Informed Performance-Based Methodology
(Event Selection, Classification, and Defense-in-Depth)

I&C Design
Architecture
Functions
Special Treatment

NEI 21-07
Safety Analysis Report Content

NRC Design Review Guide
I&C Reviews

Safety Strategy
Deterministic Methodology with Risk Insights
(Defense Lines, Classification, Event Identification, and Analysis Methods

I&C Design
Architecture
Functions
Design Rules

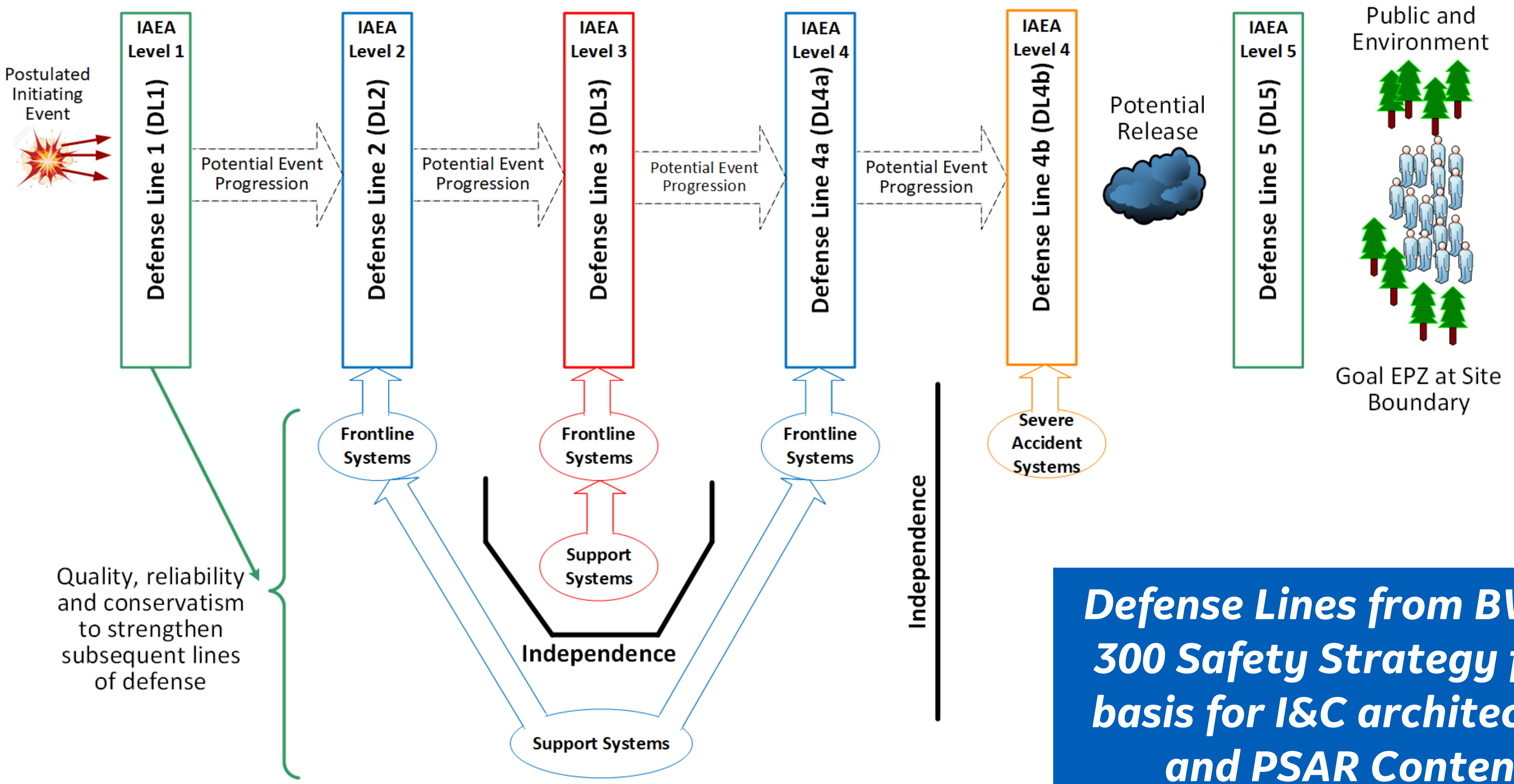
Safety Analysis Report
Optimized Alternative Format

NRC Design Review Guide
I&C Reviews

BWRX-300

HITACHI

BWRX-300 Safety Strategy – Lines of Defense



Defense Lines from BWRX-300 Safety Strategy form basis for I&C architecture and PSAR Content

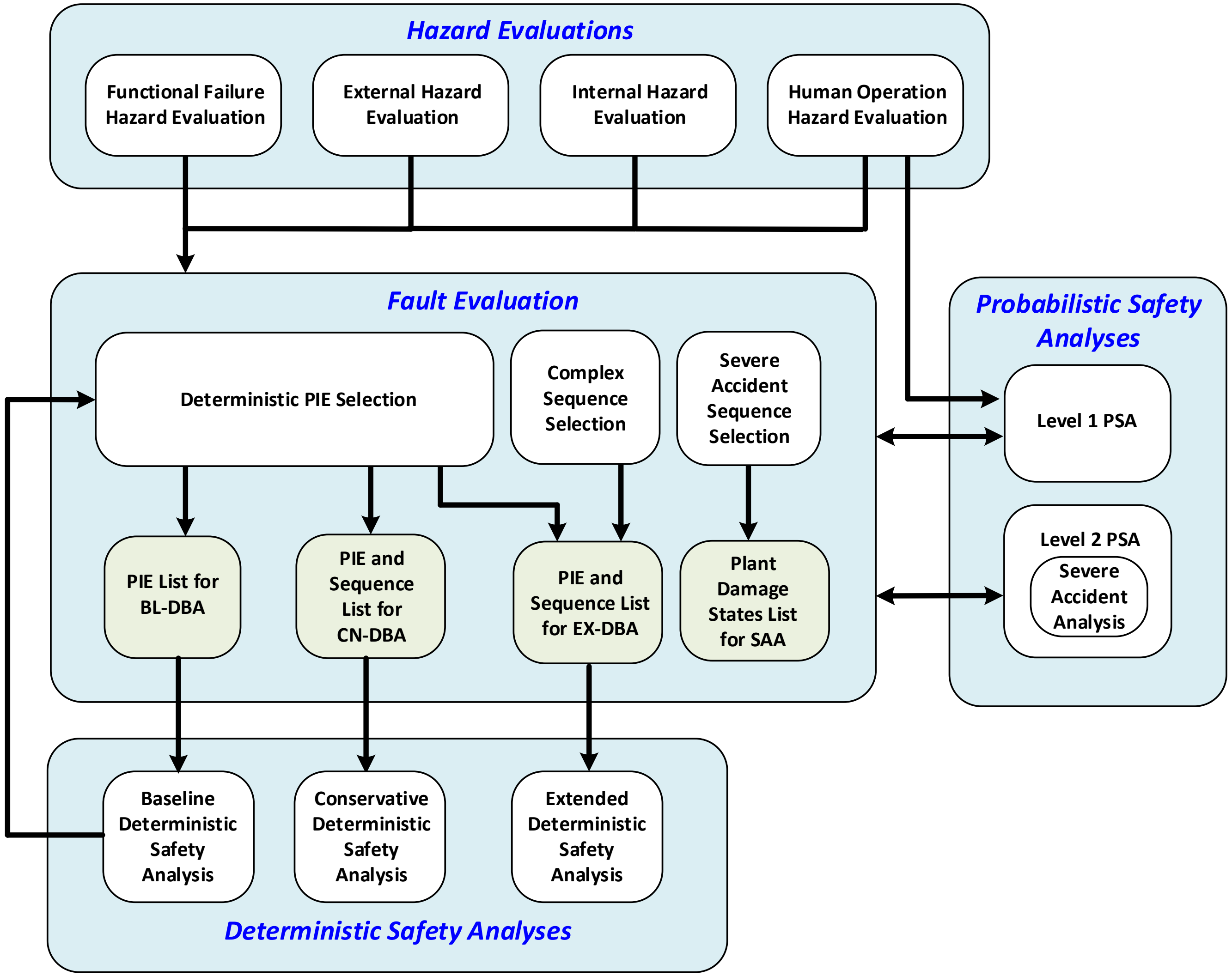
HITACHI

BWRX-300 Safety Strategy – Classification for I&C

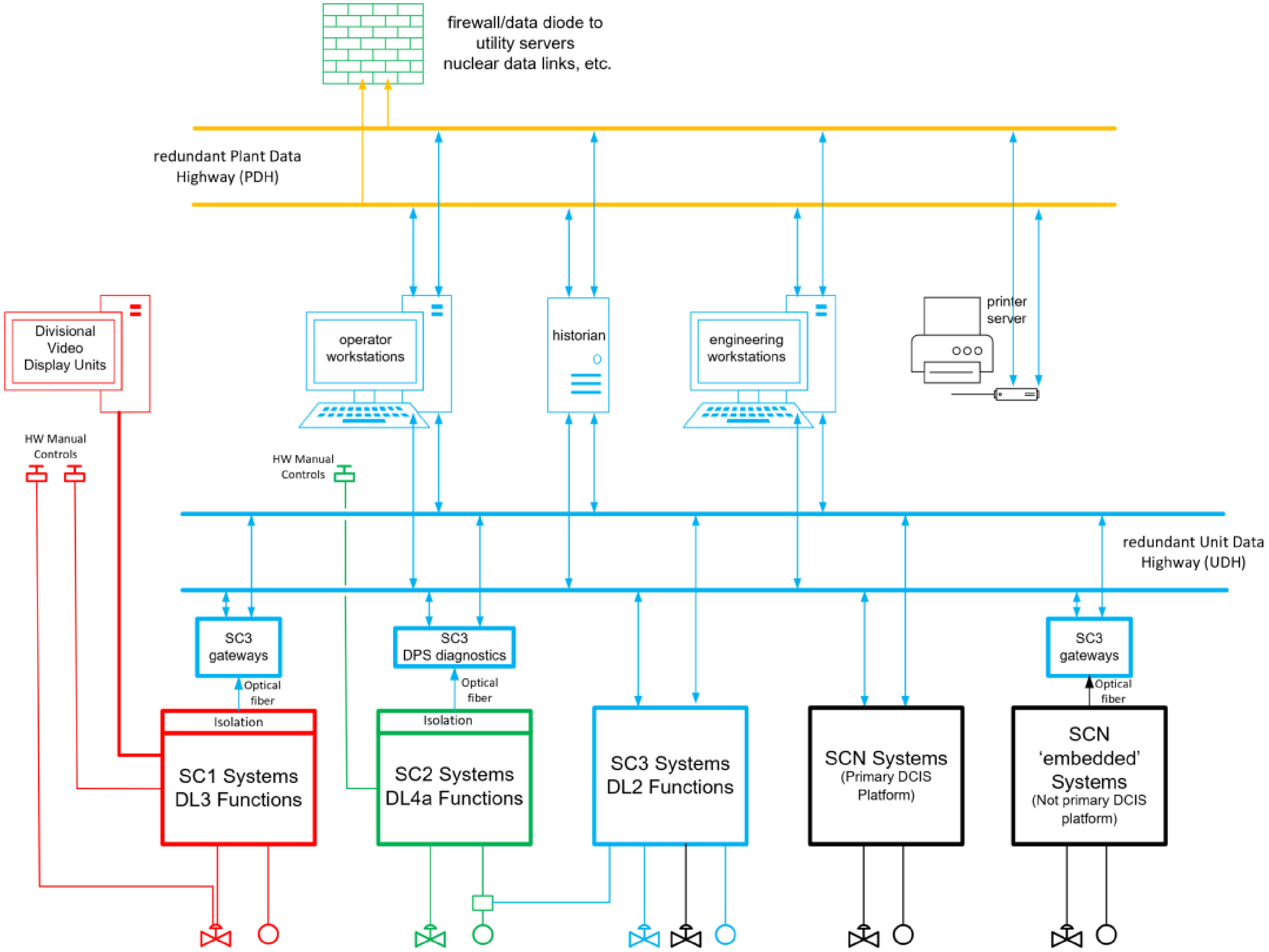
- Defense Line 3 primary safety functions are implemented in Safety Class 1 equipment
- Defense Line 4a primary safety functions are implemented in at least Safety Class 2 equipment
- Defense Line 2 primary safety function are implemented in at least Safety Class 3 equipment
- Defense Line 4b function are implemented in Safety Class 3 equipment

BWRX-300 Safety Strategy – Analysis Methodology

- Perform hazard evaluation to define initiating events
- Determine limiting sequences
- Categorize events based on probability (risk insights)
- Perform deterministic analyses
- Define Defense Line Functions



BWRX-300 I&C Architecture Concept



HITACHI

IEC Standards for BWRX-300 I&C System Design

Safety Class	Description	Systems	Equipment
SC1, SC2, and SC3	I&C Equipment supporting Safety Category 1, 2 and 3 functions (systems C10 and C20)	IEC 61513 (I&C architecture and general system requirements) IEC 60709 (separation) IEC 63147 (accident monitoring) IEC 60812 (FMEA)	IEC 61000-4, IEC 61000-6-2 (electromagnetic compatibility)
SC1	I&C Equipment supporting Safety Category 1 functions (system C10)	IEC 60880 (Category A software) IEC 60987 (hardware)	IEC 60780 (environmental) IEC 60980 (seismic) IEC 61500 (network communication)
SC2	I&C Equipment supporting Safety Category 2 functions (system C20)	IEC 60987 (hardware) IEC 62138 (Category B software)	IEC 60780 (environmental) IEC 61508
SC3	I&C Equipment supporting Safety Category 3 functions (system C20)	IEC 62138 (Category C software)	IEC 60980 (seismic) - Note 1 IEC 61508

Note 1 – If required for mitigation of seismic-related events.

HITACHI

NRC I&C Design Review Guide

DESIGN REVIEW GUIDE (DRG): INSTRUMENTATION AND CONTROLS FOR NON-LIGHT-WATER REACTOR (NON-LWR) REVIEWS

U.S. NUCLEAR REGULATORY COMMISSION

REVISION DATE: 02/26/2021

X.0 OVERVIEW OF REVIEW PROCESS

X.0.1 INTRODUCTION

As discussed in the report "Near-Term Task Force Review of Insights from the Fukushima Dai-ichi Accident," [1] the current nuclear regulatory infrastructure was developed for the purpose of reactor licensing in the 1960s and 1970s and supplemented as necessary to address significant events or new issues. To modernize the NRC regulations, the Commission has provided direction to the NRC staff to promote, among other approaches, the use of Probabilistic Risk Assessment (PRA) technology in a manner that complements the NRC's deterministic approach and supports the NRC's traditional defense-in-depth (DID) philosophy. For example, in Staff Requirements Memorandum (SRM) to SECY-11-0024, "Use of Risk Insights to Enhance the Safety Focus of Small Modular Reactor [SMR] Reviews," [2] the Commission approved the staff's recommendation to enhance the efficiency and effectiveness of the SMR application reviews through a design-specific, risk-informed, and safety-focused approach. In response to the Commission's approval, the NRC instrumentation and controls (I&C) staff developed a Design-Specific Review Standard (DSRS) Chapter 7, "Instrumentation and Controls," initially for the BWXT mPower™ SMR design and subsequently for the NuScale SMR design [3]. The restructured safety-focused approach in DSRS Chapter 7, Section 7.1, emphasized fundamental I&C design principles (i.e., independence, redundancy, diversity in support of DID, and deterministic behavior (repeatability and predictability)), and was a step forward for other future SMR and advanced non-light water reactor (non-LWR) licensing applications.

This Design Review Guide (DRG) chapter provides guidance for the NRC staff to use in reviewing the I&C portions of applications for advanced non-LWRs within the bounds of existing regulations.[1] This guidance leverages the DSRS Chapter 7 framework while factoring in the lessons learned from new reactor reviews. This guidance supports the NRC's Vision and Strategy document entitled "Safely Achieving Effective and Efficient Non-Light Water Reactor Mission Readiness," [4] and the "Non-LWR Vision and Strategy Near-Term Implementation Action Plans" [5]. Specifically, the guidance discussed herein supports Implementation Action Plan Strategy 3, which involves developing: (1) guidance for flexible regulatory review processes for non-LWRs within the bounds of existing regulations; and (2) a new non-LWR regulatory framework that is risk-informed and performance-based, and that features staff's review efforts commensurate with the demonstrated safety performance of non-LWR technologies. This DRG chapter also factors in the principles in Regulatory Guide (RG) 1.233, "Guidance for Technology-Inclusive, Risk-Informed, and Performance-Based Approach to Inform the Licensing Basis and Content of Applications for Licenses, Certifications, and Approvals for Non-Light-Water Reactors" [6]. RG 1.233 endorses the methodology in Nuclear Energy Institute (NEI) 18-04, "Risk-Informed Performance-Based Technology-Inclusive Guidance for Non-Light Water Reactor Licensing Basis Development," [7] with clarifications and points of emphasis.

SECY-19-0117, "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," [8] references RG 1.233 and provides a methodology for identifying licensing basis events (LBEs); classifying structures, systems, and components (SSCs); and assessing DID adequacy. Many vendors have indicated that they plan to use the

[1] The DRG was developed to address the immediate needs associated with the non-LWR community. Since the DRG is technology inclusive, it may be used for the review of LWR plant designs and other reactor technologies.

X-1

- DRG was well received by ACRS, and they commented it had a more universal applicability for I&C system reviews than the limitation to non-LWR reviews
- DRG allows use of either domestic standards (e.g., IEEE) or international standards (e.g., IEC)
- DRG framework aligns with BWRX-300 design philosophy for plant safety based on IAEA lines of defense and use of international standards for I&C systems

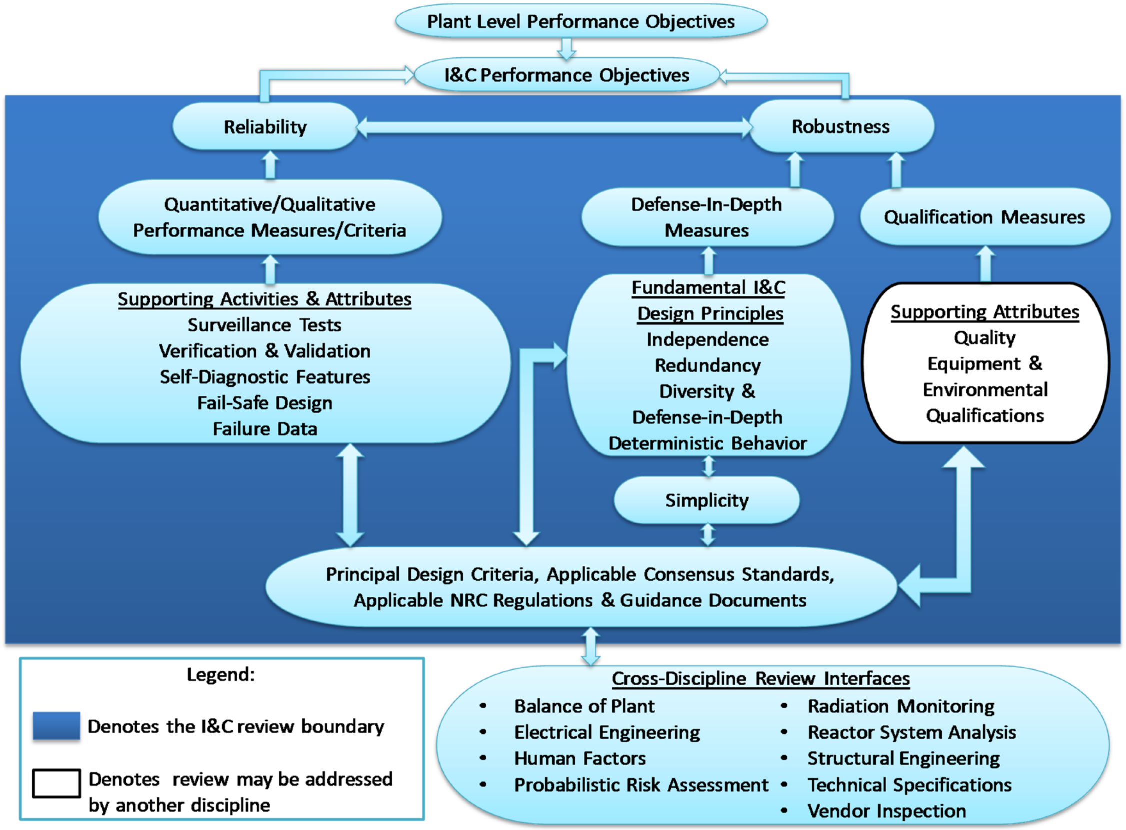
HITACHI

NRC I&C Design Review Guide Alignment with SAR

Architecture
- The NRC staff review starts at the I&C architecture level
- Ensure that the information necessary to understand the proposed I&C architecture and system functions is available

Safety-Significant Functions
- The NRC staff review focuses on safety-significant functions and selected SSCs that support them
- Ensure that the I&C performance objectives are met

Functions Not Safety-Significant
- The design-related review for SSCs that the NRC staff determined are not safety-related and not risk significant should be less
- The NRC staff review focuses on ensuring that failure or operation of such SSCs will not prevent other SSCs from performing their safety-significant functions or adversely affect DID adequacy



Alternate SAR Format and Content Optimized to Address Design Review Guide Flow and Topics

HITACHI

Insights

- IEC standards used, as allowed by the DRG, and directly align with BWRX-300 defense line classifications
- IEC standards support I&C architecture and system development process in an integrated manner that also aligns with DRG information flow
- Alternate SAR Format is used to align with DRG information flow and content
- BWRX-300 Safety Strategy framework requires some alternative Preliminary Design Criteria to align with BWRX-300 Defense Lines

HITACHI

Alternate Framework Discussions

- Some advanced reactor vendors are planning on using alternate frameworks for licensing basis event selection and SSC classification
- The following presentations are intended to communicate <u>examples</u> of how these processes impact digital I&C
- Any discussion of the use of alternate frameworks is intended to address generic issues on the impact of alternate frameworks on digital I&C licensing decisions

Questions – Alternative Frameworks

In determining I&C design criteria required to prevent or mitigate the effects of Anticipated Operational Occurrences, SRP Chapter 15 Section I.4 states:

> *The reviewer ensures that the application lists the settings of all the **protection and safety systems functions that are used (i.e., credited) in the safety evaluation**. Typical protection and safety systems functions include reactor trips, isolation valve closures, ECCS initiation and ECCS. In evaluations of AOOs and postulated accidents, the performance of each credited protection or safety system is required to include the effects of the most limiting single active failure. [emphasis added]*

NEI 18-04 Table 3-1 states:

> *AOOs take into account the expected response of **all SSCs within the plant, regardless of safety classification**. [emphasis added]*

Questions – Alternative Frameworks

Historically, there has been a perception that an applicant needs a safety-related system, instead of a set of anticipatory and/or non-safety SSCs, in order to meet AOO acceptance criteria.

Question 1: If a vendor proposes to use an alternative framework, can that vendor credit the expected response of all SSCs within the plant (e.g., other than safety-related instrumentation and controls), regardless of safety classification?

Questions – Alternative Frameworks

Question 2: If the vendor is able to credit the expected response of all SSCs within the plant, this will impact the selection and wording of Principal Design Criteria. Are there any specific considerations that vendors should be aware of when applying this concept?

For example, 10 CFR 50, Appendix A GDC 20 states:

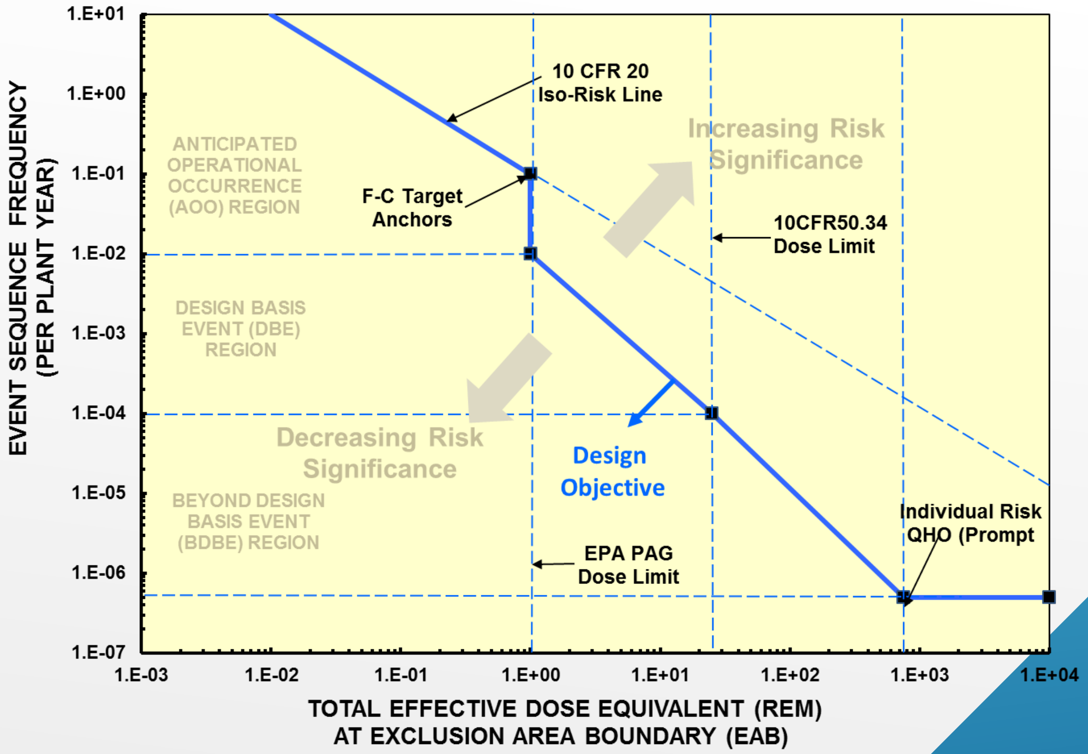
> *Protection system functions. The protection system shall be designed (1) to initiate automatically the operation of appropriate systems including the reactivity control systems, to assure that specified acceptable fuel design limits are not exceeded as a result of anticipated operational occurrences and (2) to sense accident conditions and to initiate the operation of systems and components important to safety.*

The highlighted words may be defined and executed differently in different frameworks.

Open Discussion

Perspectives on Design Basis Accident (DBA) Analysis Described in the Licensing Modernization Project (LMP)

LMP: EVENT SELECTION; F-C CURVE



- LBEs are defined by event sequence families from design specific Probabilistic Risk Assessment (PRA)
- Purpose is to evaluate risk significance of individual LBEs and SSCs and to help define the required safety functions (RSFs); not a regulatory acceptance criterion
- Derived from the NGNP F-C Target and frequency bins for event categories
- F-C Target anchor points based on:
  - 10 CFR 20 annual dose limits used to define iso-risk contour in AOO region
  - Avoidance of offsite protective actions for lower frequency AOOs
  - 10 CFR 50.34 dose limit for lowest frequency DBEs
  - Consequences based on 30day TEDE dose at EAB
  - EAB dose target for BDBEs related to NRC safety goal for limiting possibility of prompt fatality

LMP: EVENT SELECTION & ANALYSIS

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. **Event sequences with mean frequencies of 1×10^{-2}/plant-year and greater are classified as AOOs. AOOs take into account the expected response of all SSCs within the plant, regardless of safety classification.**

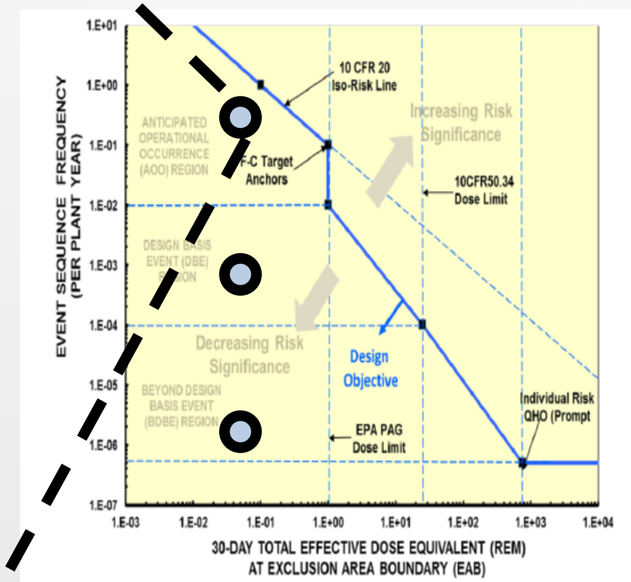


Figure 3-1. Frequency-Consequence Target

LMP: EVENT SELECTION & ANALYSIS

Design Basis Events (DBEs)

Infrequent **event sequences** that are not expected to occur in the life of a nuclear power plant, which may include one or more reactor modules, but are less likely than AOOs**. Event sequences with mean frequencies of 1×10^{-4}/plant-year to 1×10^{-2}/plant-year are classified as DBEs. DBEs take into account the expected response of all SSCs within the plant regardless of safety classification.**

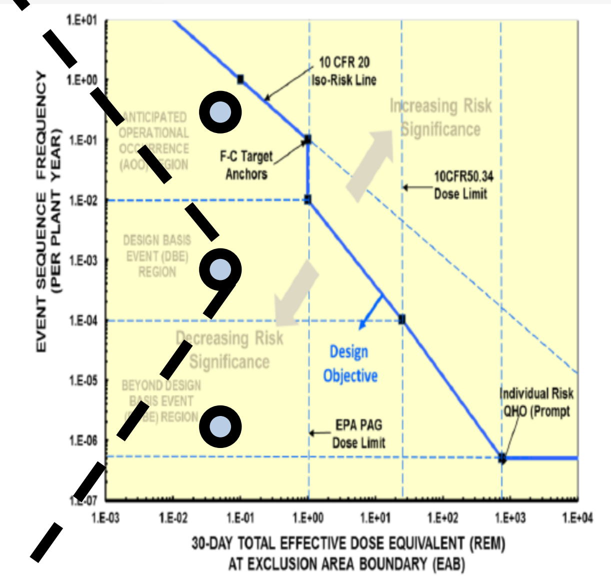


Figure 3-1. Frequency-Consequence Target

LMP: EVENT SELECTION & ANALYSIS

Beyond Design Basis Events (BDBEs)

Rare **event sequences** that are not expected to occur in the life of a nuclear power plant, which may include one or more reactor modules, but are less likely than a DBE. **Event sequences with mean frequencies of 5×10^{-7}/plant-year to 1×10^{-4}/plant-year are classified as BDBEs. BDBEs take into account the expected response of all SSCs within the plant regardless of safety classification.**

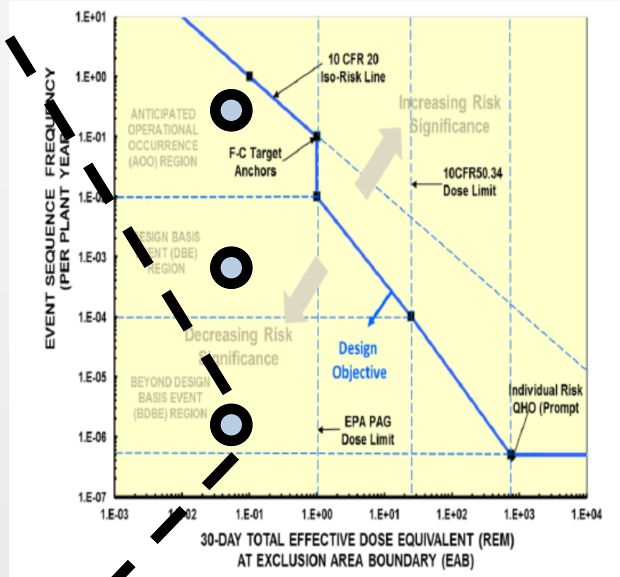


Figure 3-1. Frequency-Consequence Target

LMP: REQUIRED SAFETY FUNCTIONS (RSF)

Required Safety Function: A PRA Safety Function that is required to be fulfilled to maintain the consequence of one or more DBEs or the frequency of one or more high-consequence BDBEs inside the F-C Target

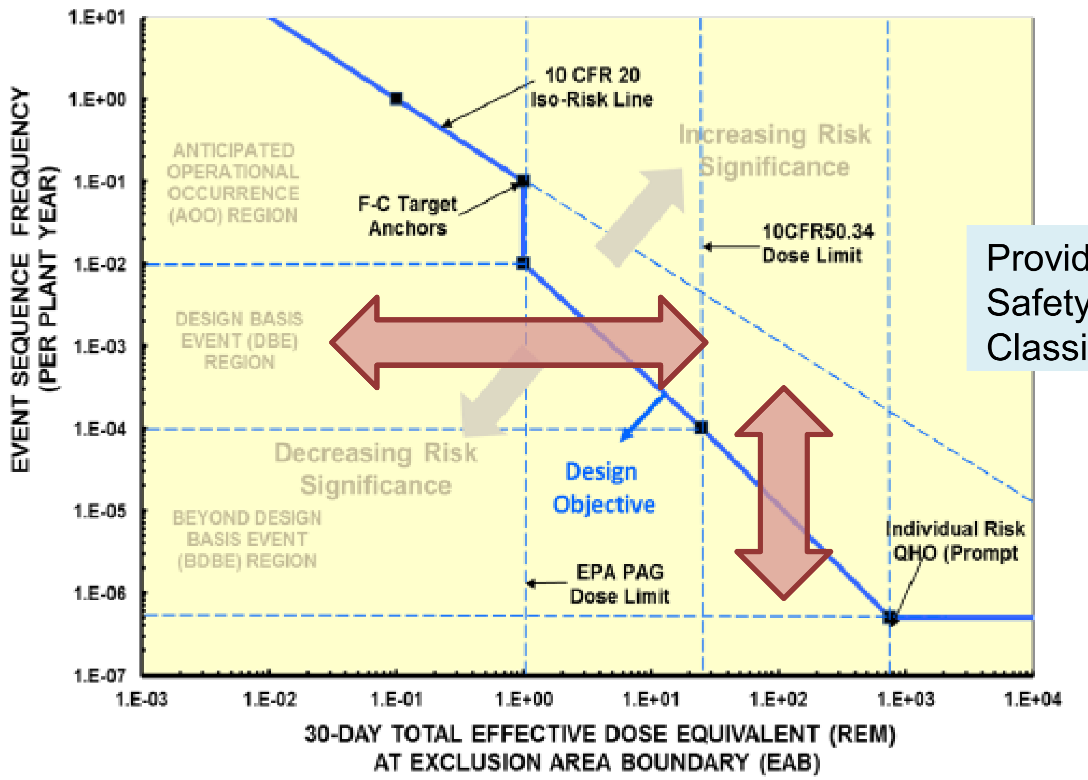


Figure 3-1. Frequency-Consequence Target

Provides connection to Safety-Related Classification

LMP: SAFETY-RELATED SSCS

- SSCs selected by the designer from the SSCs that are available to perform the RSFs to mitigate the consequences of DBEs to within the LBE F-C Target, and to mitigate DBAs that only rely on the SR SSCs to meet the dose limits of 10 CFR 50.34 using conservative assumptions

- SSCs selected by the designer and relied on to perform RSFs to prevent the frequency of BDBE with consequences greater than the 10 CFR 50.34 dose limits from increasing into the DBE region and beyond the F-C Target

LMP: DESIGN BASIS ACCIDENTS

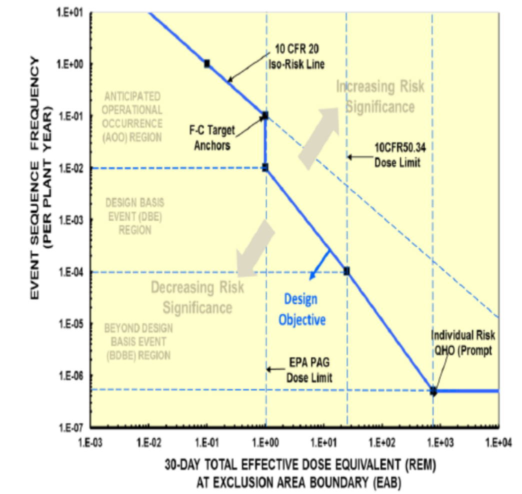


Figure 3-1. Frequency-Consequence Target

Design Basis Accidents (DBAs)

Postulated event sequences that are used to set design criteria and performance objectives for the design of Safety-Related SSCs. DBAs are derived from DBEs based on the capabilities and reliabilities of Safety-Related SSCs needed to mitigate and prevent event sequences, respectively. **DBAs are derived from the DBEs by prescriptively assuming that only Safety-Related SSCs are available to mitigate postulated event sequence consequences to within the 10 CFR 50.34 dose limits.**

LMP: DESIGN BASIS ACCIDENTS

- A DBA is associated with each DBE that includes the required safety function (RSF) challenges.
  - DBAs selected based on prescriptive rules and analyzed using conservative assumptions.
  - In DBA analysis, RSFs are performed by Safety-Related SSCs only.
- The selection of conservative assumptions to be used in the DBA analysis will be informed by the quantitative uncertainty analysis of consequences performed for the corresponding DBEs.
- The application of a single failure criterion is deemed unnecessary. Replaced with reliability criterion.
  - Based primarily on integrated LMP methodology. Alternate approaches would need to maintain or justify not applying single failure criterion for DBAs.
- NRC Regulatory Guide 1.203, "Transient and Accident Analysis Methods"
  - Additional discussion of developing appropriate evaluation models for analyzing DBAs.

Future Workshop Topics

- Follow-on Questions / Discussion related to the LMP DBA Analysis
- Codes and Standards
  - How performance-based concepts can be applied to prescriptive requirements of endorsed codes and standards
  - Applicability of IEEE 603 and related standards
  - Use of international codes and standards

Future Workshop Topics

- NRC staff review expectations
  - I&C-specific Principal Design Criteria
  - Fundamental I&C design principles
  - I&C architecture and safety classification of I&C platforms
- Content of Applications
  - Clarity on applicability of Part 50/52 requirements
  - Expectation for construction permit applications
  - Non-power vs. power reactor applications
    - Use of NUREG-1537; Path forward for future power reactors

Questions?

For more information, contact:

Jordan.Hoellman2@nrc.gov