TerraPower

NATRIUM

I&C Defense-in-Depth and Diversity Strategy

a TerraPower & GE-Hitachi technology

NAT-3313

Table of Contents

- Natrium™ Reactor Overview
- Safety Case Methodology
- Licensing Basis Event Selection
- Defense-in-Depth Adequacy
- I&C Support of Natrium Safety Case
- Next Interactions

TerraPower NATRiUM

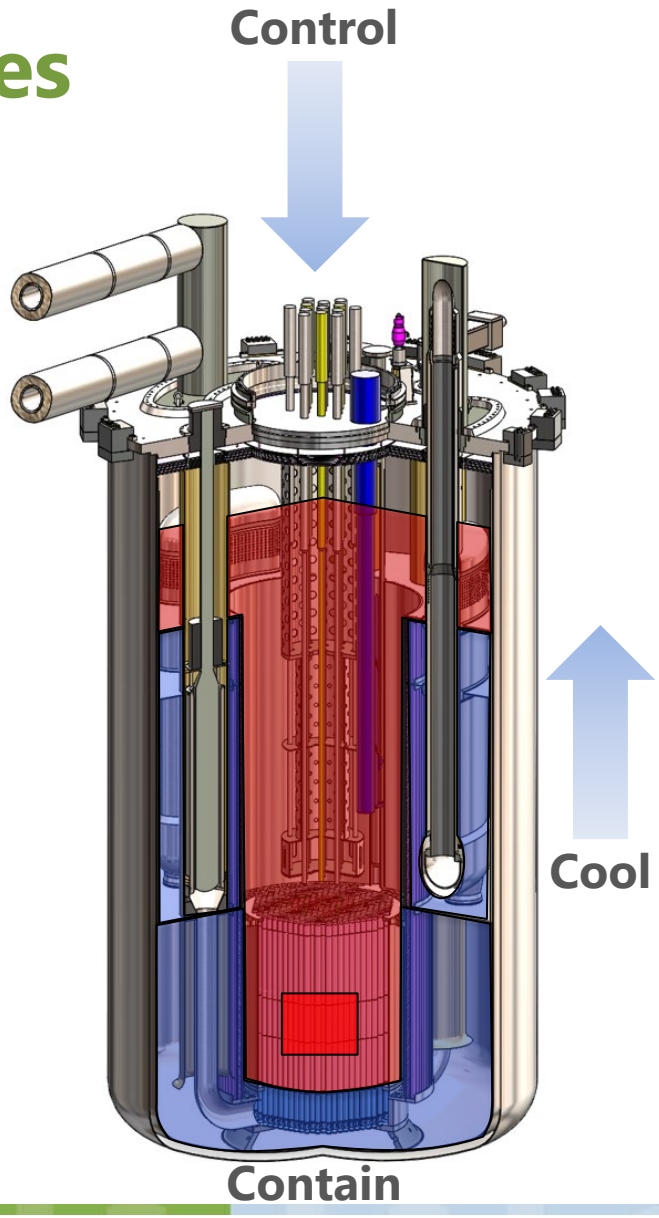
Natrium Reactor Overview

- The Natrium project is demonstrating the ability to design, license, construct, startup and operate a Natrium reactor.

- Pre-application interactions are intended to reduce regulatory uncertainty and facilitate the NRC's understanding of the Natrium design and its safety case.

Natrium Safety Features

- Pool-type Metal Fuel SFR with Molten Salt Energy Island
  - Metallic fuel and sodium have high compatibility
  - No sodium-water reaction in steam generator
  - Large thermal inertia enables simplified response to abnormal events
- Simplified Response to Abnormal Events
  - Reliable reactor shutdown
  - Transition to coolant natural circulation
  - Indefinite passive emergency decay heat removal
  - Low pressure functional containment
  - No reliance on Energy Island for safety functions
- No Safety-Related Operator Actions or AC power
- Technology Based on U.S. SFR Experience
  - EBR-I, EBR-II, FFTF, TREAT
  - SFR inherent safety characteristics demonstrated through testing in EBR-II and FFTF



Control

- Motor-driven control rod runback and scram follow
- Gravity-driven control rod scram
- Inherently stable with increased power or temperature

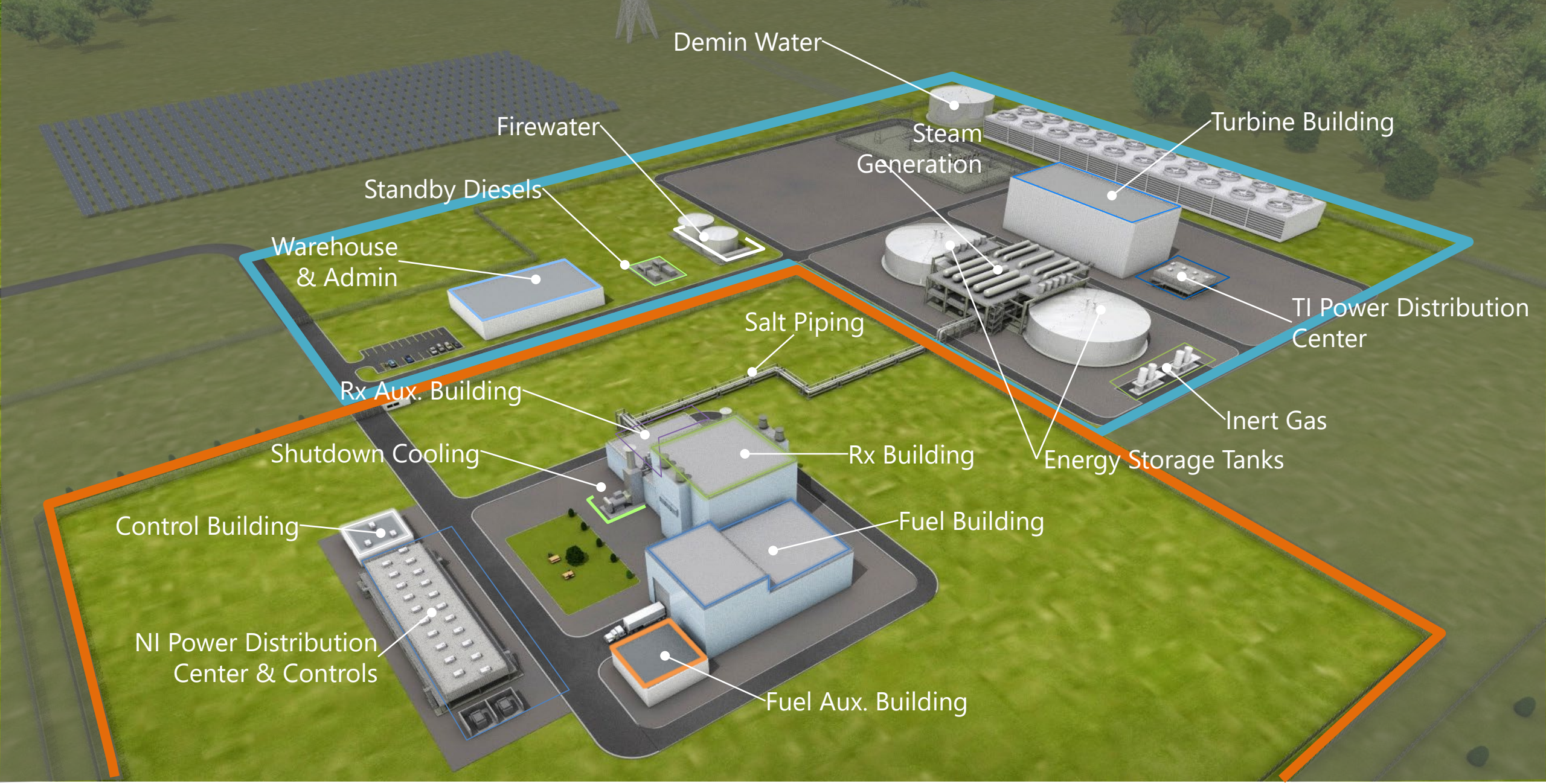
Cool

- In-vessel primary sodium heat transport (limited penetrations)
- Intermediate air cooling natural draft flow
- Reactor air cooling natural draft flow – always on

Contain

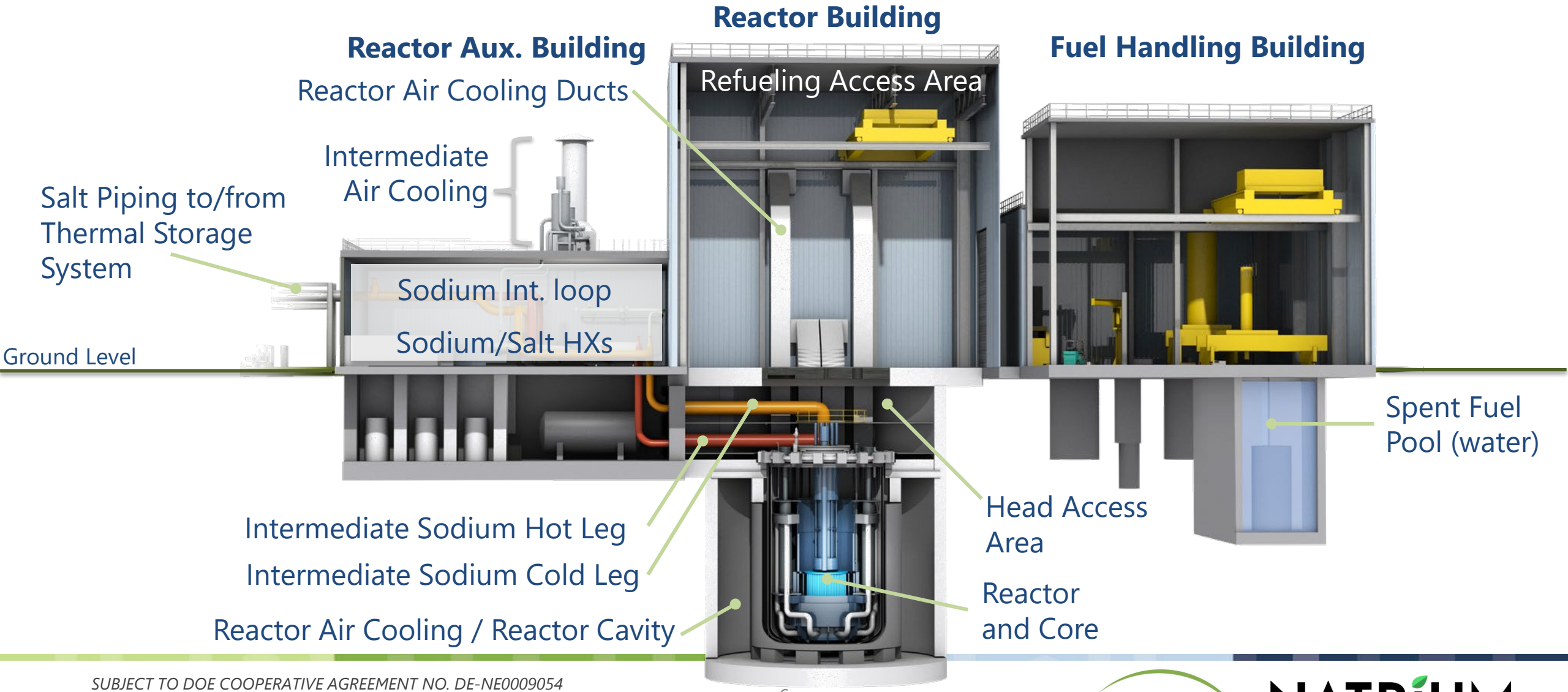
- Low primary and secondary pressure
- Sodium affinity for radionuclides
- Multiple radionuclides retention boundaries

TerraPower NATRIUM



TerraPower NATRIUM

Plant Overview



TerraPower NATRIUM

SAFETY CASE METHODOLOGY

Safety Case Methodology Interface with I&C

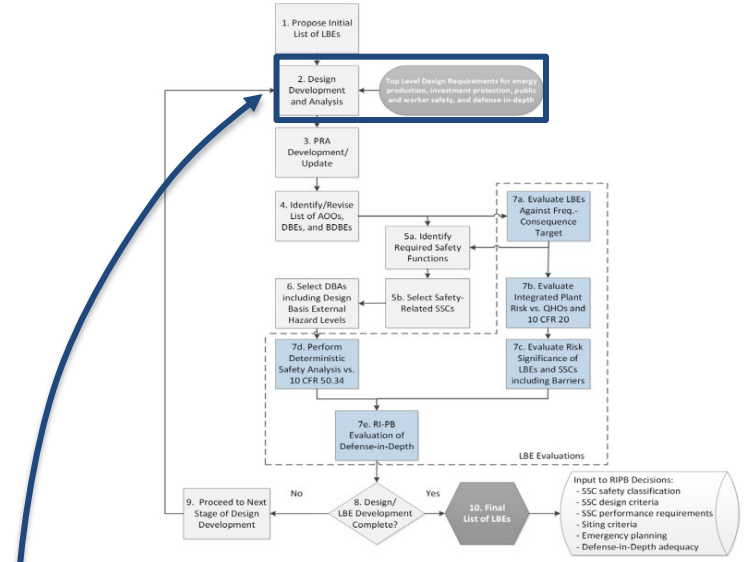
- Whole plant evaluation of DID ensures adequate reliability and performance of safety functions
- I&C Implements a variety of specific safety functions which are part of the whole plant evaluation
- RPS reliability goal is set to keep failures out of the Design Basis Event range which involves the same features that would typically be used to demonstrate CCF prevention

Safety Case Methodology

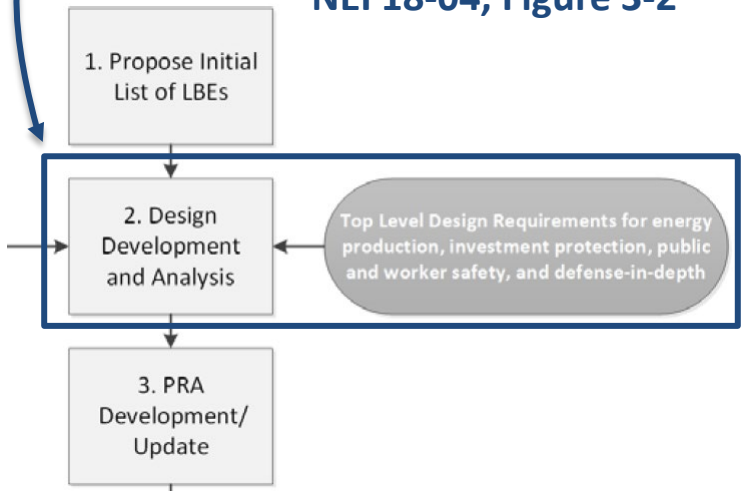
- Natrium safety case is derived from the NEI 18-04 licensing basis development process, as endorsed by RG 1.233
- An integrated, iterative process facilitates LBE selection, SSC safety classification, and determination of DID adequacy
  - There are direct connections between PRA, LBE selection, faulted events, and deterministic safety analysis that quantify safety functions
  - The IDPP makes the final judgment on SSC classifications taking consideration for any missing scope or limitation in the PRA
- Development of I&C systems includes design features for meeting criteria of defensive levels, PRA reliability targets, and assumptions

Safety Case Methodology

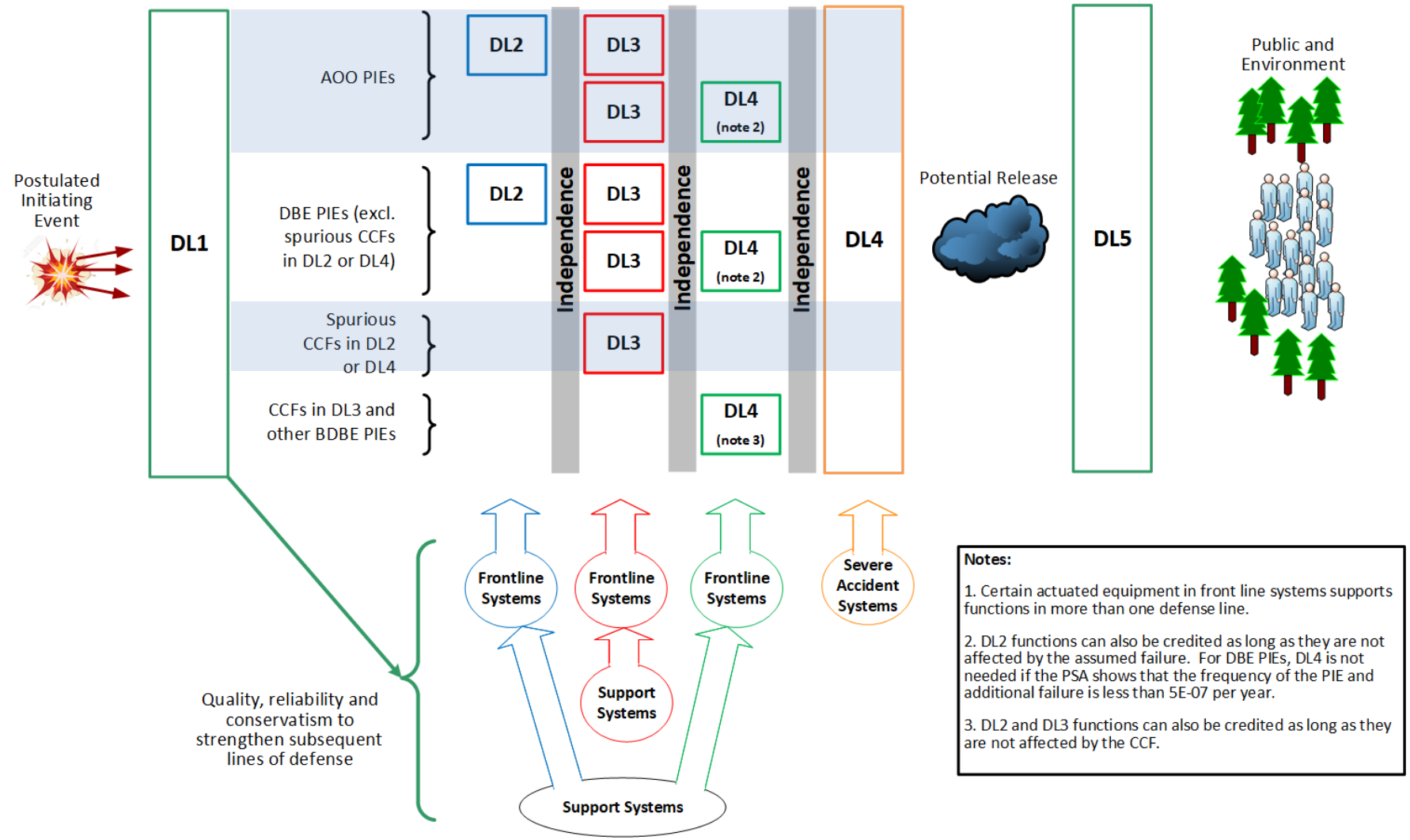
- Design team is applying an explicit DL approach consistent with IAEA SSR-2/1 DL definitions:
  - Identification of mitigating functions for each LBE
  - Assignment of functions to DLs
  - Confirmation of two functional DLs capable of mitigating AOO or most DBE initiating events
  - Application of independence and diversity requirements between functional DLs
- Supports early indications of safety classifications:
  - DL3 functions 'match' SR assignment in LMP
  - DL4 functions align with NSRST assignment in LMP but with some expected differences
  - In some cases, a DL2 function may align with NSRST
- This approach is intended to minimize the number of needed design iterations and decreases opportunity for 'surprises' when the RIPB Evaluation of DID Adequacy step is performed



NEI 18-04, Figure 3-2



Safety Case Methodology



Notes:

1. Certain actuated equipment in front line systems supports functions in more than one defense line.

2. DL2 functions can also be credited as long as they are not affected by the assumed failure. For DBE PIEs, DL4 is not needed if the PSA shows that the frequency of the PIE and additional failure is less than 5E-07 per year.

3. DL2 and DL3 functions can also be credited as long as they are not affected by the CCF.

TerraPower NATRIUM

Safety Case Methodology

- PRA being used during the design phase to inform design decisions and provide risk insights
- PRA Methods Report developed which follows the current version of the Non-LWR PRA Standard (ASME/ANS RA-S-1.4-2021)
- PRA scope developed and documented:
  - Internal Events At-Power PRA
  - Low-Power/Shutdown Internal Events PRA
  - Scoping Seismic, High Winds, Flood, and Fire PRAs

LICENSING BASIS EVENT SELECTION

Previous NRC Engagements Related to LBE Selection

- Probabilistic Risk Assessment and application of Licensing Modernization Project (July 2021)
- Risk-informed, performance-based SSC classification (Oct 2021)
- Functional containment (March 2022)
- Emergency Planning Zone methodology (Aug 2022)
- Principal Design Criteria (Dec 2021, Nov 2022)
- Event Selection and Evaluation (Jan 2023)

Process for Selecting and Evaluating Events

- Process follows NEI 18-04 to select Licensing Basis Events
- Meets requirements of ASME/ANS RA-S-1.4-2021
- DID considerations or regulatory requirements may introduce events otherwise screened out on a quantitative basis
  - Examples: reactor vessel leak, aircraft impact
- Plant Event database is used
  - Traceability of event selection and disposition is important for both establishing and meeting requirements

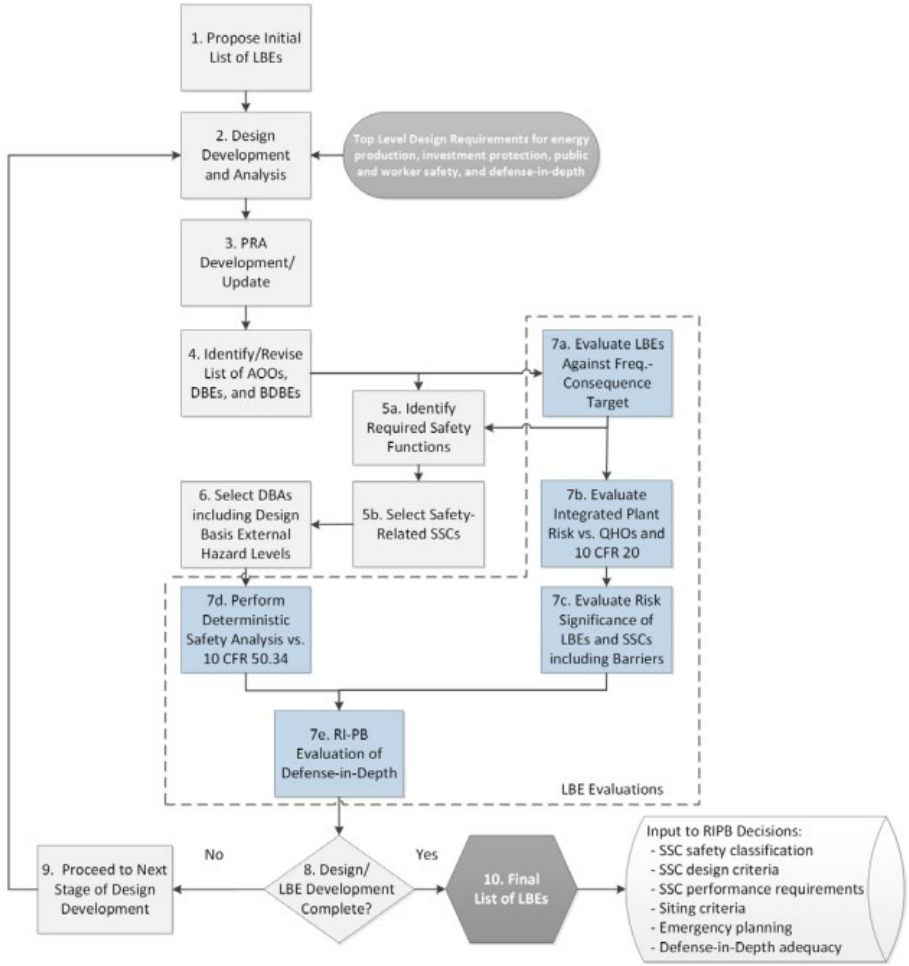
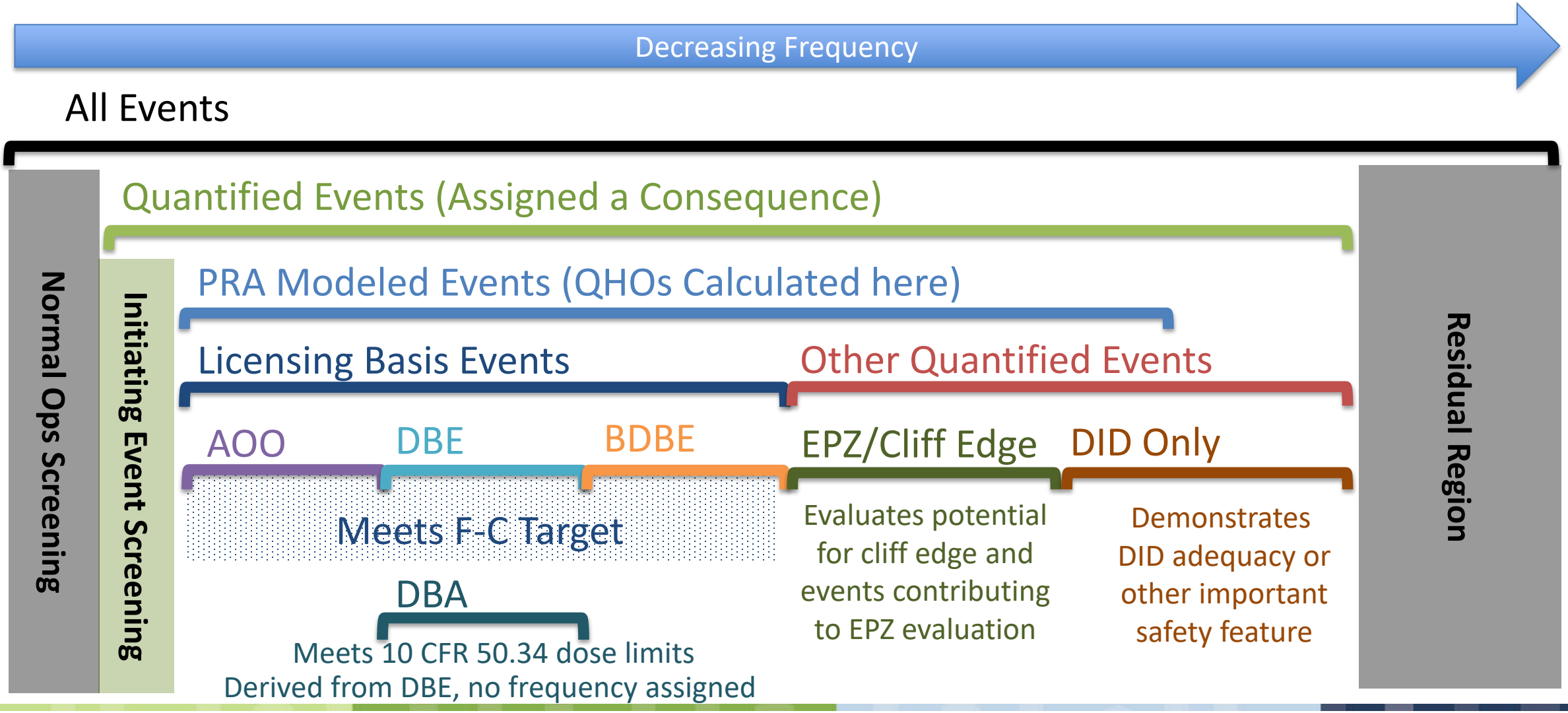


Figure 3-2 from NEI 18-04: Process for Selecting and Evaluating Licensing Basis Events

Event Type Line Diagram by Frequency



TerraPower NATRIUM

DBA Selection

- DBAs are derived from the list of DBEs by prescriptively assuming that only SR SSCs are available to mitigate postulated event sequence consequences to within the 10 CFR 50.34 dose limits
  - The required safety functions are initially defined in step 5a, if a DBA derived from this list of functions doesn't meet the dose limit as evaluated in step 7d, iterate by returning to step 5a
- This process is completed for all DBEs and may result in the combination of multiple DBEs into a single DBA if the safety related systems credited result in the same event progression

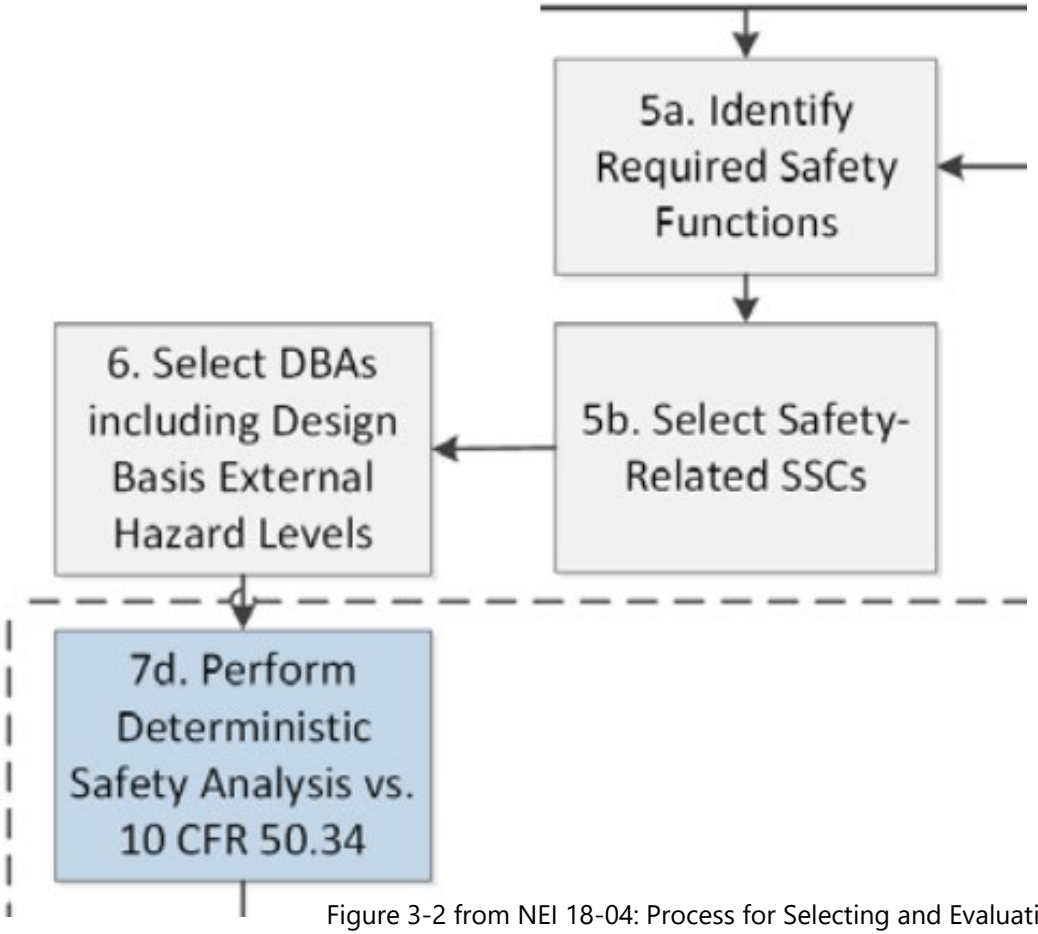


Figure 3-2 from NEI 18-04: Process for Selecting and Evaluating Licensing Basis Events

DEFENSE-IN-DEPTH ADEQUACY

Defense-in-Depth Adequacy

- DL1 includes programmatic elements and design features
  - Minimize potential for IEs to occur in the first place, and
  - Minimize potential for failures to occur in subsequent DLs
- DL2 is the normal response to most postulated initiating events
  - DL2 functions are classified as NST, with some exceptions being classified as NSRST
- DL3 is sufficient to mitigate all DBAs/DBEs
  - DL3 functions are classified as SR
- DL4 is for BDBEs or to provide required or supplemental DID
  - DL4 functions are classified as NSRST, with some exceptions being classified as NST
- DL5 is related to emergency planning

Defense-in-Depth Adequacy

- Baseline analyses: Evaluate plant response to AOO and DBE PIEs assuming all plant functions perform as designed
  - Preferably uses only DL2 functions; DL3 can be used
  - Design basis for DL2 functions
- Conservative analyses: Evaluate plant response to AOO and DBE PIEs assuming DL2 functions fail
  - Must use only DL3 functions
  - Design basis for DL3 functions
- Extended analyses: Evaluate plant response to BDBE PIEs
  - Must use DL4 functions when AOO PIE was not mitigated by DL2 alone in Baseline analysis
  - Must use DL4 functions when DBE PIE was not mitigated by DL2 alone in Baseline analysis, and it was not mitigated to frequency less than 5E-7 in Conservative analysis
  - Any DL2 or DL3 function not failed as part of the PIE or that are uncredited in the baseline or conservative analysis may also be used
- Event list of AOOs, DBE, and BDBEs is interface between safety/PRA analysis and design activities to identify preventive and mitigative functions and assign them to DLs

Defense-in-Depth Adequacy

- IDPP Review of DID ensures:
  - Scope of PRA is sufficiently complete
  - LBEs and SSCs are identified adequately
  - Basis of RSF selection is sound
  - SR SSCs can perform RSFs appropriately
  - Protective measures for risk-significant LBEs are well understood
  - Protective measures against CCF are identified
  - Any available risk benefit is characterized; e.g., sensitivity studies to determine if more margin can be achieved easily

DID Evaluation Considerations – Plant Capability, Risk Informed

- Comprehensive review of PRA uncertainty and margins are considered in the DID adequacy evaluation
- Knowledge, performance, model, and completeness uncertainties are considered
- Evaluations showing performance and risk margin demonstrate there are not phenomenological or risk cliff-edges
- PRA screening assessments performed in determining scope are reviewed to confirm appropriate consideration for uncertainties and margin

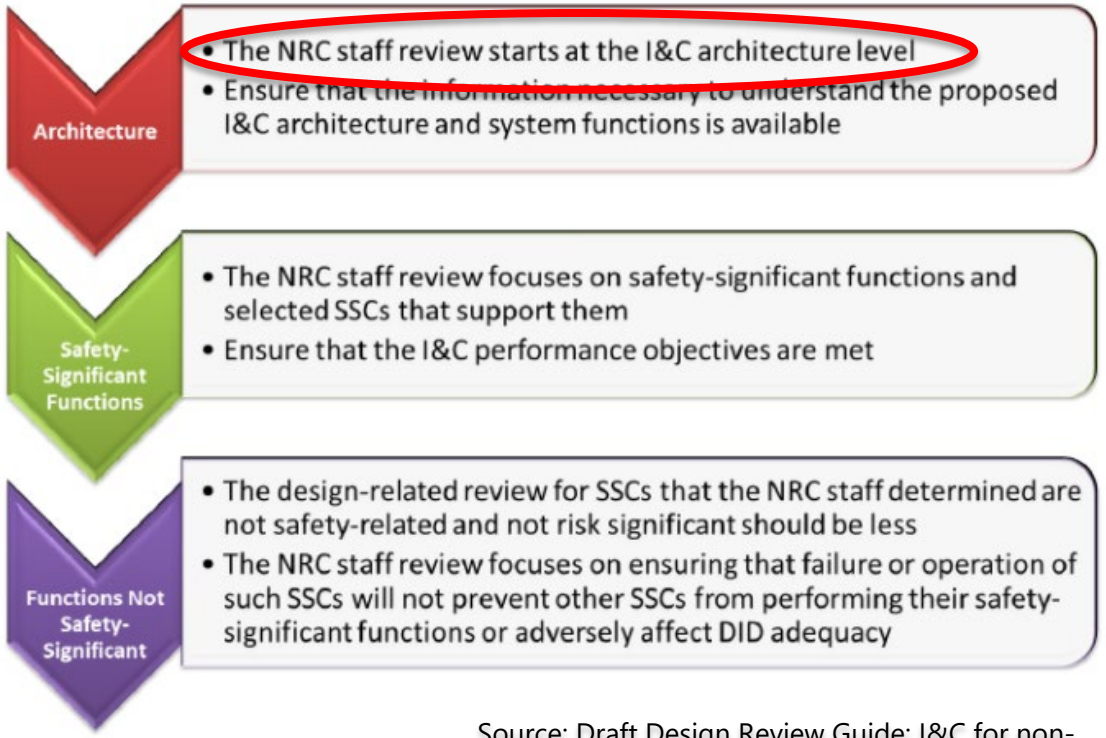
I&C SUPPORT OF NATRIUM SAFETY CASE

I&C Support of Natrium Safety Case

- SSC support of the safety case is achieved through assignment of safety classifications
- Assignment of SSC safety classifications is a result of allocation of plant-level functions to SSCs
- Plant-level functions are decomposed for allocation to plant systems and to the I&C Architecture
- I&C Architecture is further decomposed for function allocation to specific I&C systems

I&C Support of Natrium Safety Case

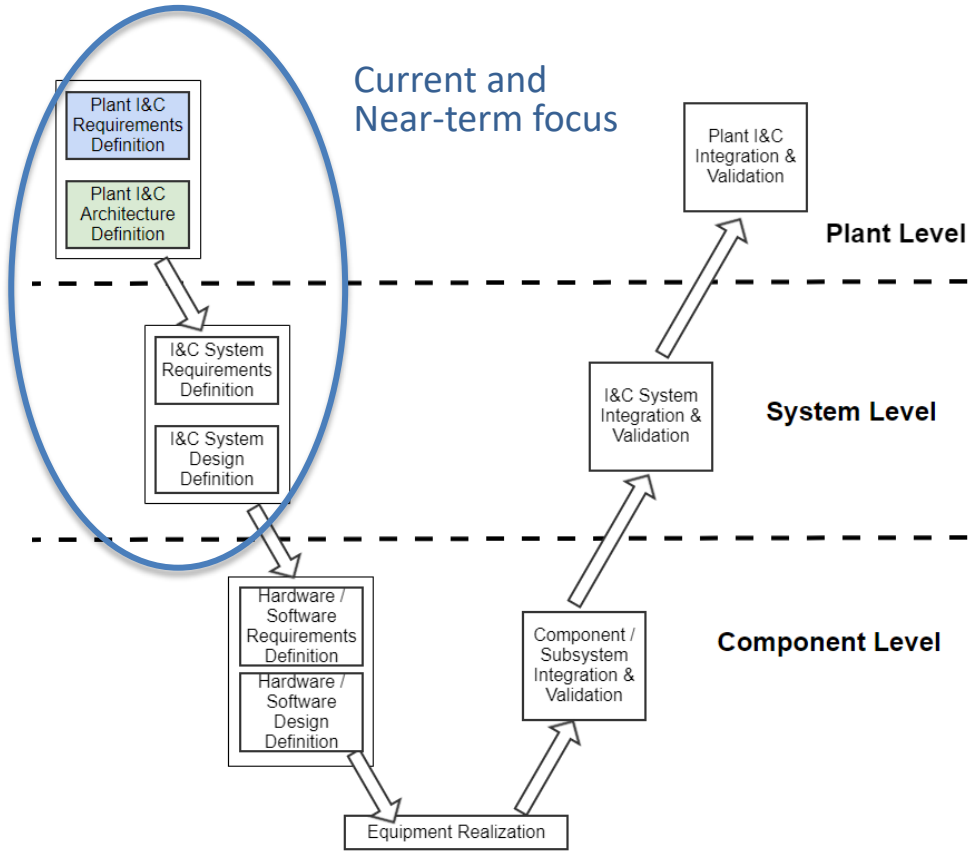
- The Plant I&C Architecture is the organizational structure of the I&C systems in the plant
- Organizational structure comprises definition of each I&C system in terms of its:
  - Assigned functions
  - Safety classifications, and
  - Relationships to other systems (including communication between I&C systems)
- The fundamental design principles of independence, diversity, redundancy, and simplicity are first applied to the Plant I&C Architecture (not to individual I&C systems; the I&C systems are constrained by application of these principles at the plant-level)



Source: Draft Design Review Guide: I&C for non-LWR Reviews, Figure X-2

I&C Support of Natrium Safety Case

- Plant-level I&C architecture translates plant-level functions, performance objectives, and constraints into I&C system requirements
- Current focus is on requirements definition and architecture design
  - Preliminary plant level requirements have been developed
  - I&C systems have been defined
  - Function allocation in progress (iterative process)



I&C Support of Natrium Safety Case

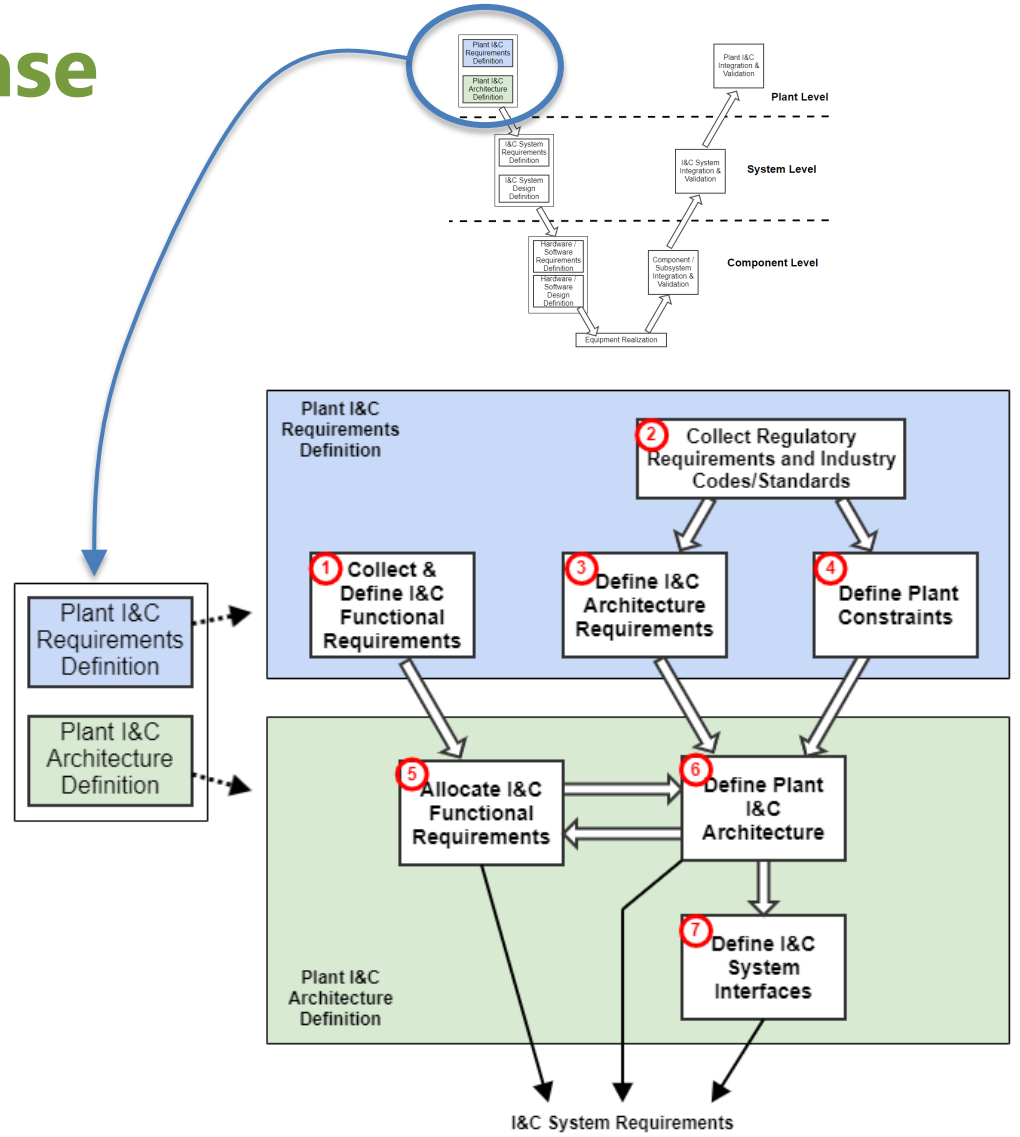
1. I&C Functional Requirements

   Define the necessary functions to control, operate and/or monitor a defined part of the plant process
2. Regulatory Requirements, Codes and Standards

   Identify those that are applicable, scope of applicability, and derivation of project/design-specific requirements to implement
3. Architecture Requirements

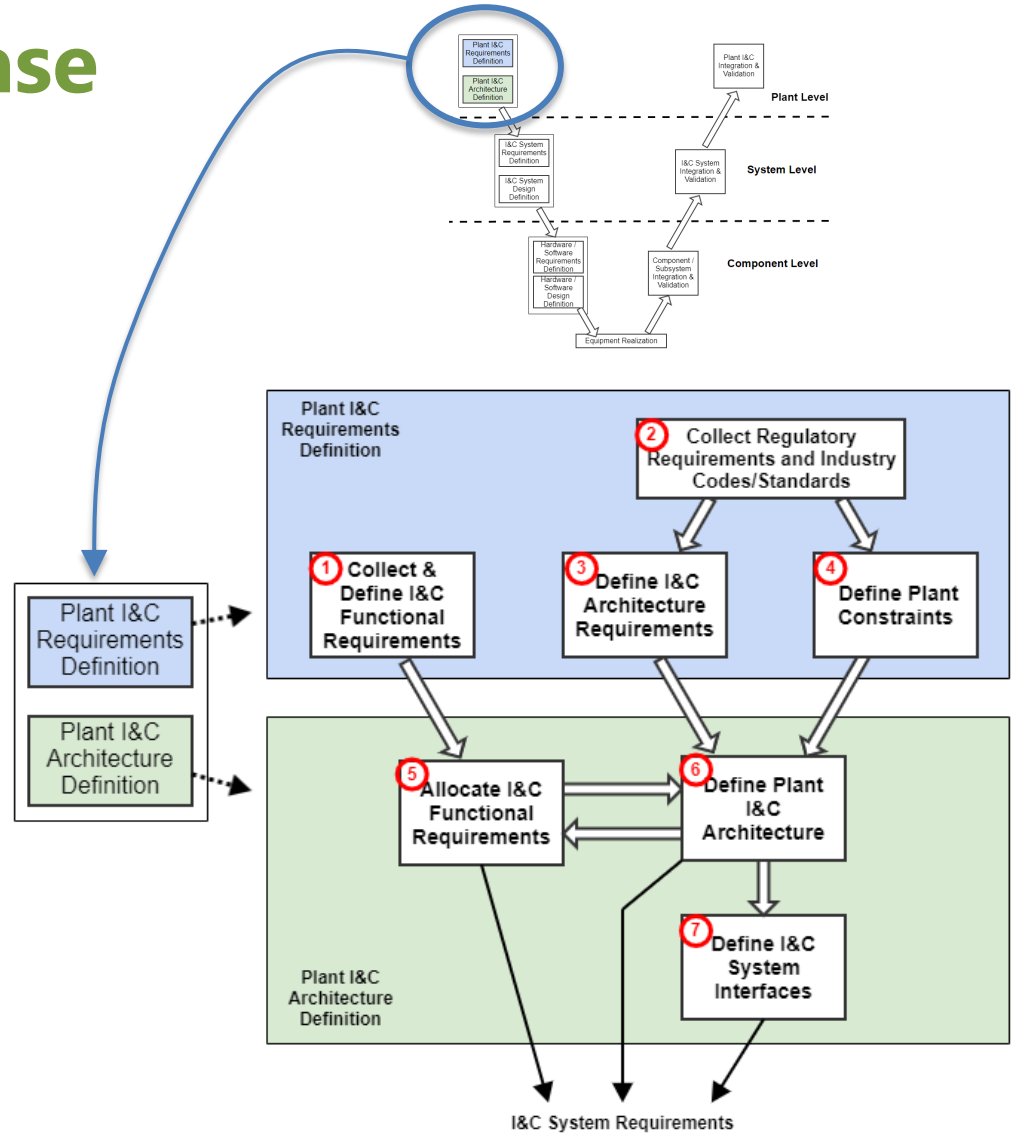
   Define the requirements that determine which I&C systems must be independent and/or diverse from each other and levels of redundancy for each I&C system
4. Plant Constraints

   Identify constraints placed on the I&C from 'external' influences, such as; building and room layouts, environmental conditions, human factors, cyber security, process system interfaces, and on-line maintenance approaches



I&C Support of Natrium Safety Case

5. Allocate I&C Functional Requirements
   - Decompose I&C functions and allocating to I&C sub-systems and components
   - Define interfaces between I&C systems
6. Define Plant I&C Architecture to Establish the Definition of Each I&C System Including its:
   - Design basis functions
   - Position among the DLs
   - Safety Classification
   - Implementing technologies (technology platform)
   - Necessary interfaces
   - Physical location in the plant
7. I&C Interfaces
   - Establish specific requirements to govern implementation of interfaces between I&C systems



I&C System Diversity

- The potential for CCF is addressed by the chosen platform
  - Per BTP 7-19, no further consideration of diversity is needed
- D3 analysis will address CCF of digital sensors for SR functions, if any
  - CCF of sensors can be addressed by PRA & reliability target, 100% testing for simple devices, and/or use of different type or manufacturer
- I&C design includes the following features to further support the plant DID:
  - Failure modes and hazards are identified and mitigated
    - Hazard analysis includes assessment of fault propagation from non-safety to safety systems, and impact on the plant safety and safety functions
  - The I&C platforms are chosen based on performance, quality, and reliability goals
  - I&C systems are segregated
  - As needed, additional functional segregation is implemented within system(s) based on failure modes, hazards analysis, and the plant level DID input
  - Manual reactor trip function

I&C Systems Performance

- Performance measures are established for Safety Significant systems to meet the PRA and DID analysis safety goals, including:
  - Design development (including design processes)
  - Manufacturing and construction
  - Operational and maintenance programs
- To achieve adequate DID, the I&C architecture and systems design meet the fundamental I&C design principles and simplicity, consisting of:
  - independence,
  - redundancy,
  - diversity, and
  - deterministic behavior (predictability and repeatability)
- The I&C systems are assigned to a specific defensive level based on their main function; however, systems may perform functions at a different level (e.g., manual reactor scram is DL-4 but assigned to RPS system)
  - DL 2: NST, allocated to NIC (some functions maybe NSRST)
  - DL 3: SR, allocated to RPS, XIS, or RIS (inputs from different systems)
  - DL 4: NSRST and NST, generally allocated to NIC
  - DL 5: Emergency planning, includes PAM (functionality resides on other systems)

SR Performance and Reliability

- SR systems are designed to QAPD QL-1, IEEE Std. 603 and IEEE Std. 7-4.3.2 (where applicable)
- RPS design considerations include:
  - Four independent divisions
  - Demonstrated reliability of 10^{-5}
  - FMEA and hazards analysis
  - Isolation of non-safety interfaces
  - RPS platform internal diversity
  - Self-diagnostics and test features
  - Fail safe design
  - Equipment qualification
  - Highest software integrity level
  - Defined design process
  - Simplicity

NSRST Performance and Reliability

- NSRST systems are designed to QAPD QL-2
- Special treatment of NSRST systems include the following, as applicable:
  - Equipment qualification (e.g., Seismic and EMC)
  - Demonstrated reliability to meet PRA goals
  - Included in maintenance program
  - Included in reporting program
  - Performance requirements related to specific NSRST function
  - Isolation of non-safety interfaces to safety systems
  - Graded software integrity level
  - Self-diagnostics and test features
  - Evaluation of faults to ensure faults do not propagate to safety systems
  - Redundant network and processors
  - Application of regulatory requirements, guidance, and industry codes and standards (e.g., RG 1.97, IEEE 497)

Programmatic Special Treatments

- Programmatic special treatments are applied to SR and NSRST systems, as applicable, to ensure PRA performance goals continue to be met. These include, but are not limited to:
  - Engineering Assurance
  - Organizational and human factors
  - Technical specifications
  - Construction and start-up programs
  - Maintenance and monitoring of SSC performance programs
  - Quality Assurance Program
- See NEI 18-04 Table 5-7 for additional examples

Conclusion

- D3 assessment is applied to the entire plant
- CCF is considered, as applicable, for different event scenarios
- The PRA required reliability goals, assumptions, and performance are met by the I&C SSC design and development
- The I&C D3 report will include:
  - Event selection and D3 assessment methodology
  - I&C systems performance in support of D3

NEXT INTERACTIONS

Next Interactions

- I&C Architecture and Design Basis Meeting, June 2023
- Fuel Handling Supervisory Control System I&C Meeting, July 2023
- Defense-in-Depth and Diversity Strategy ToR, November 2023

TerraPower NATRIUM

Acronym List

AOO – Anticipated Operational Occurrence
ANS – American Nuclear Society
ASME – American Society of Mechanical Engineers
Aux. – Auxiliary
BDBE – Beyond Design Basis Events
CCF – Common Cause Failure
CFR – Code of Federal Regulations
DBA – Design Basis Accident
DBE – Design Basis Events
DID – Defense-in-Depth
DL – Defense Line
DOE – U.S. Department of Energy
EMC – Electromagnetic Compatibility
Excl – Excluding
F-C – Frequency Consequence
FMEA – Failure Modes and Effects Analysis
GE – General Electric
I&C – Instrumentation and Controls
IAEA – International Atomic Energy Agency
IDPP – Integrated Decision-Making Process Panel
IE – Initiating Event
IEEE - Institute of Electrical and Electronics Engineers
LBE – Licensing Basis Event
LLC – Limited Liability Corporation
LMP – Licensing Modernization Project
NEI – Nuclear Energy Institute
NI – Nuclear Island
NIC – Nuclear Island Integrated Control System
NSRST – Non-safety Related with Special Treatment
NST – No Special Treatment
NQA – Nuclear Quality Assurance
PAM – Post Accident Monitoring System
PIE – Postulated Initiating Events
PRA – Probabilistic Risk Assessment
QAPD – Quality Assurance Program Description
QHO – Quantitative Health Objectives
QL – Quality Level
RG – Regulatory Guide
RIPB – Risk Informed Performance Based
RIS – Reactor Instrumentation System
RPS – Reactor Protection System
RSF – Required Safety Function
RX - Reactor
SIL – Software Integrity Level
SR – Safety Related
SSC – Structures, Systems, and Components
SSR – Specific Safety Requirements
TI – Turbine Island
TM – Trademark
ToR – Topical Report
XIS – Nuclear Instrumentation System