TerraPower

NATRIUM

Digital Instrumentation and Controls

a TerraPower & GE-Hitachi technology

SUBJECT TO DOE COOPERATIVE AGREEMENT NO. DE-NE0009054

Objectives

- Natrium™ Reactor Overview
- Simplified Safety Case - I&C Implications
- Defense-in-Depth Concept
- Plant I&C Architecture
- Design Review Guide: I&C for Non-LWR
- Safety Related I&C Vendor Selection Process
- Cyber Security Program

Natrium Reactor Licensing Overview

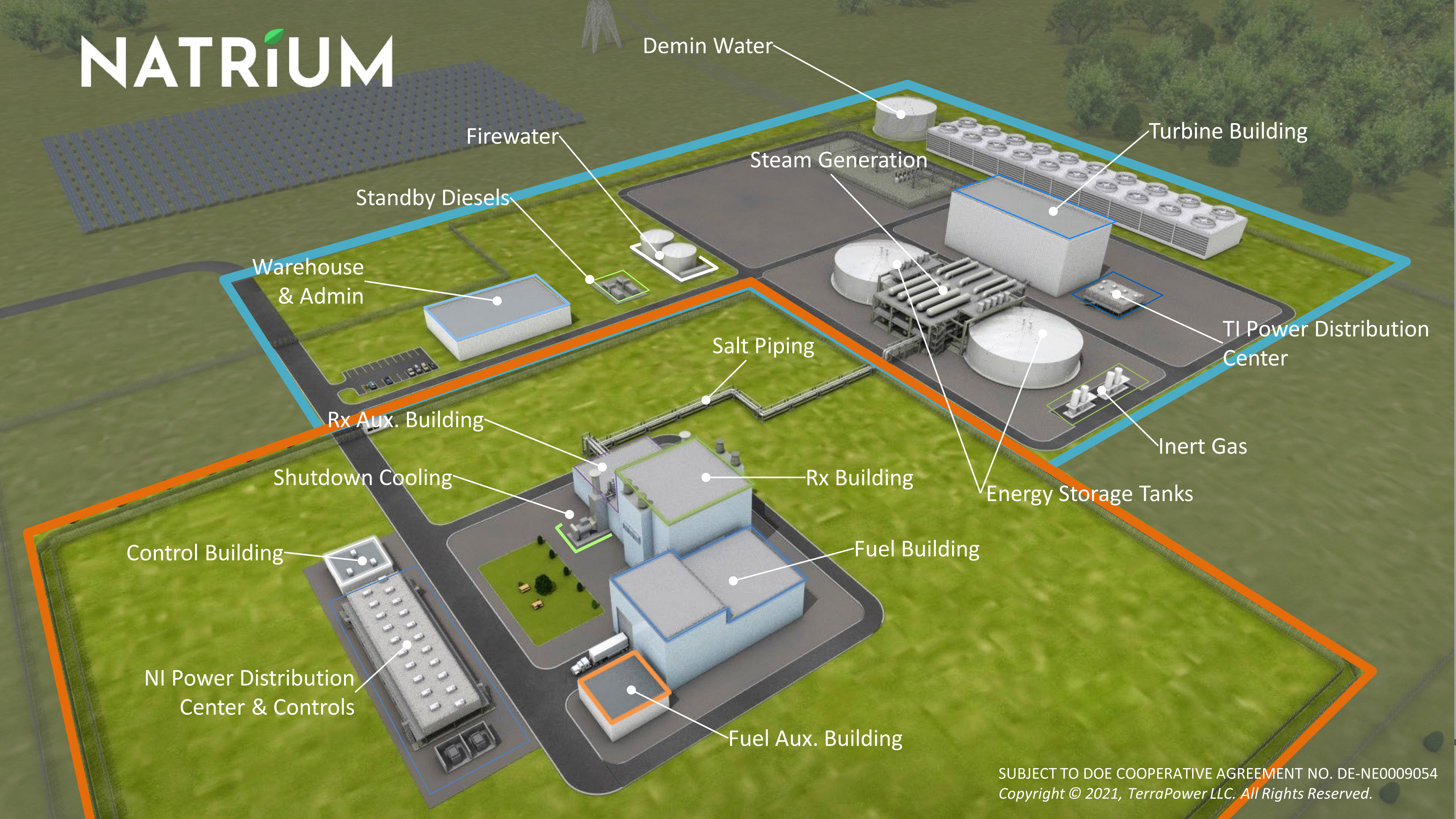
- Regulatory Engagement Plan submitted 6/8/2021
- 10 CFR 50 licensing process will be followed
  - Construction Permit Application 8/2023
  - Operating License Application 3/2026
- Numerous pre-application interactions are planned to reduce regulatory uncertainty and facilitate the NRC's understanding of Natrium technology and its safety case
- The Licensing Modernization Project (LMP) (NEI 18-04), as endorsed by RG 1.233, will support this application

Natrium Reactor Licensing Overview

- Each pre-application interaction will build upon risk insights from prior interactions to demonstrate the Natrium reactor's safety case.
- Future Meetings and Presentations include:
  – Risk-Informed, Performance-Based Principal Design Criteria
  – Energy Island Decoupling Strategy
  – Testing Plan and Methodology

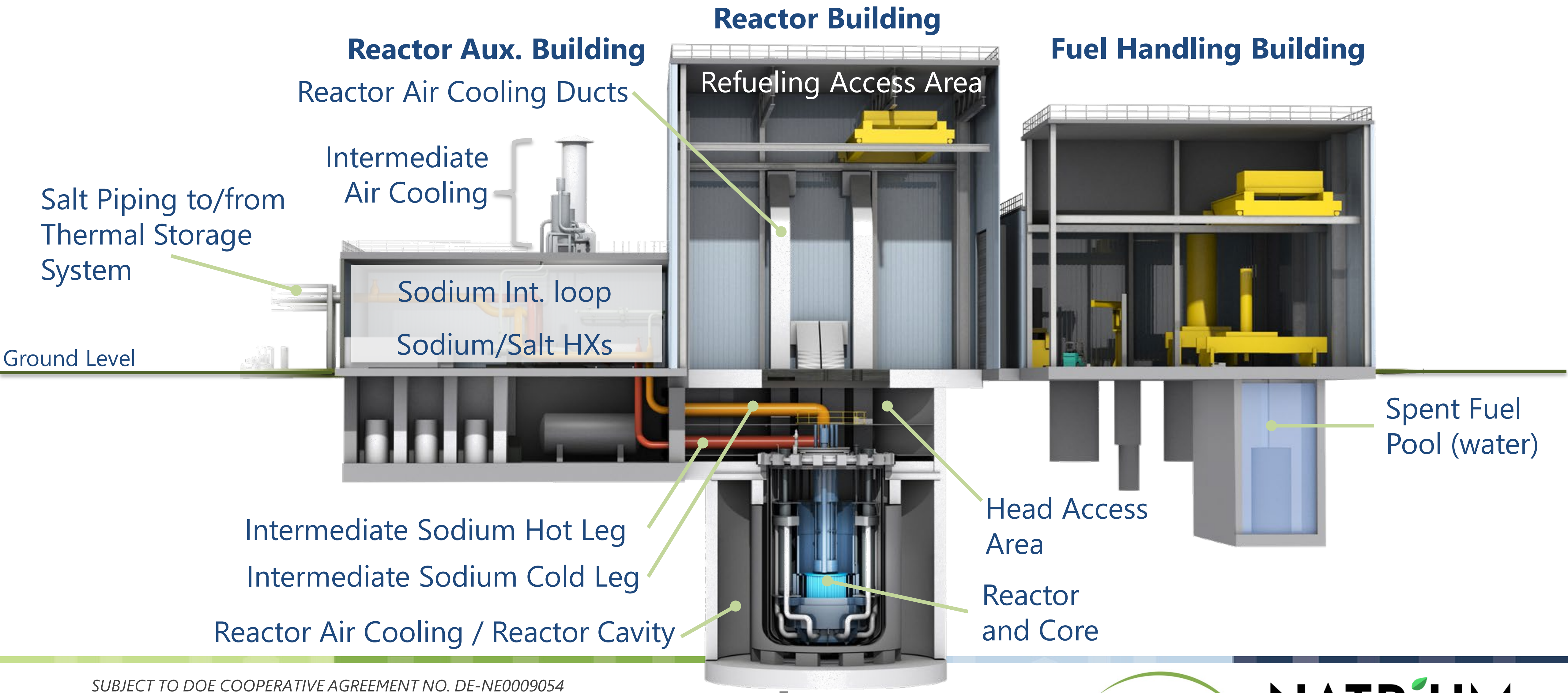
Advanced Reactor Demonstration Program

- Demonstrate the ability to design, license, construct, startup and operate the Natrium reactor within the Congressionally mandated seven-year timeframe
- Include improvements in safety, security, economics, and environmental impacts
- Utilize a simple, robust, reliable, and proven safety profile
- Lower emissions by initiating the deployment of a fleet of Natrium reactors – Demonstrate that the plants can be built economically and that they will be attractive for future owner/operators



SUBJECT TO DOE COOPERATIVE AGREEMENT NO. DE-NE0009054

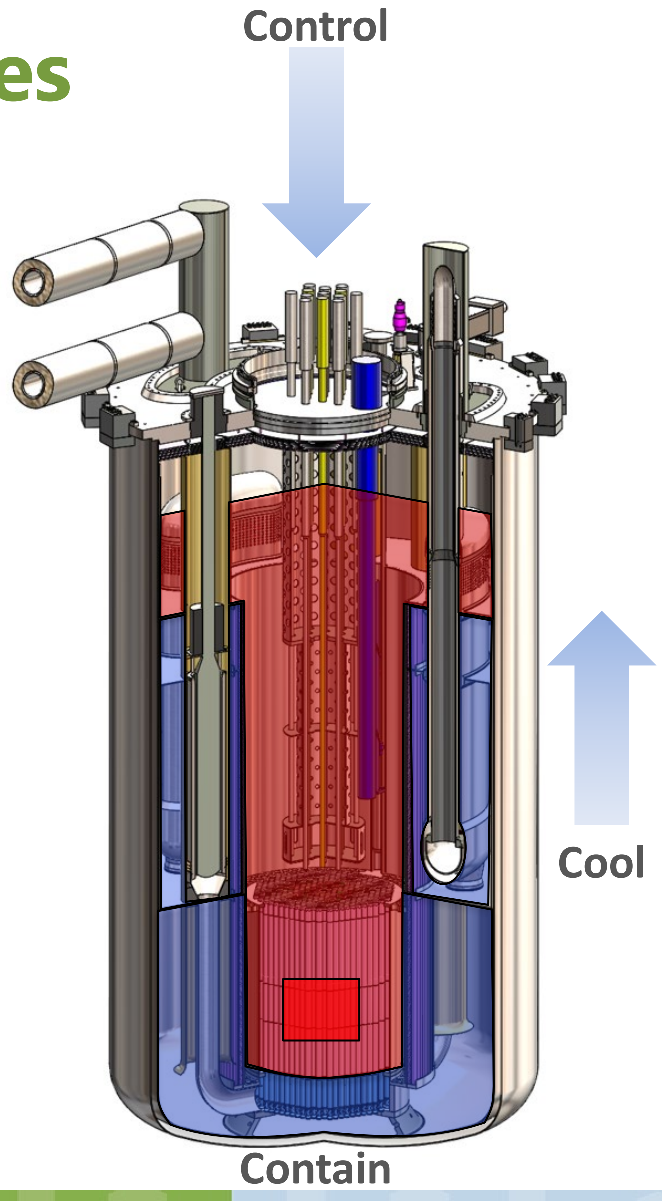
Plant Overview



TerraPower NATRIUM

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
- 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

SUBJECT TO DOE COOPERATIVE AGREEMENT NO. DE-NE0009054

TerraPower NATRIUM

Simplified Safety Case – I&C Implications

- *Design Review Guide: I&C for Non-LWR Reviews* (ML20238B936) highlights the importance of simplicity in the I&C review

> *"Simplicity of the design will facilitate the NRC staff's efficient assessment of the safety of the I&C design"*

> *"The staff considers simplicity to be a cross-cutting concept that supports the fundamental I&C design principles discussed in Section X.0.1.1 for developing I&C systems with high reliability."*

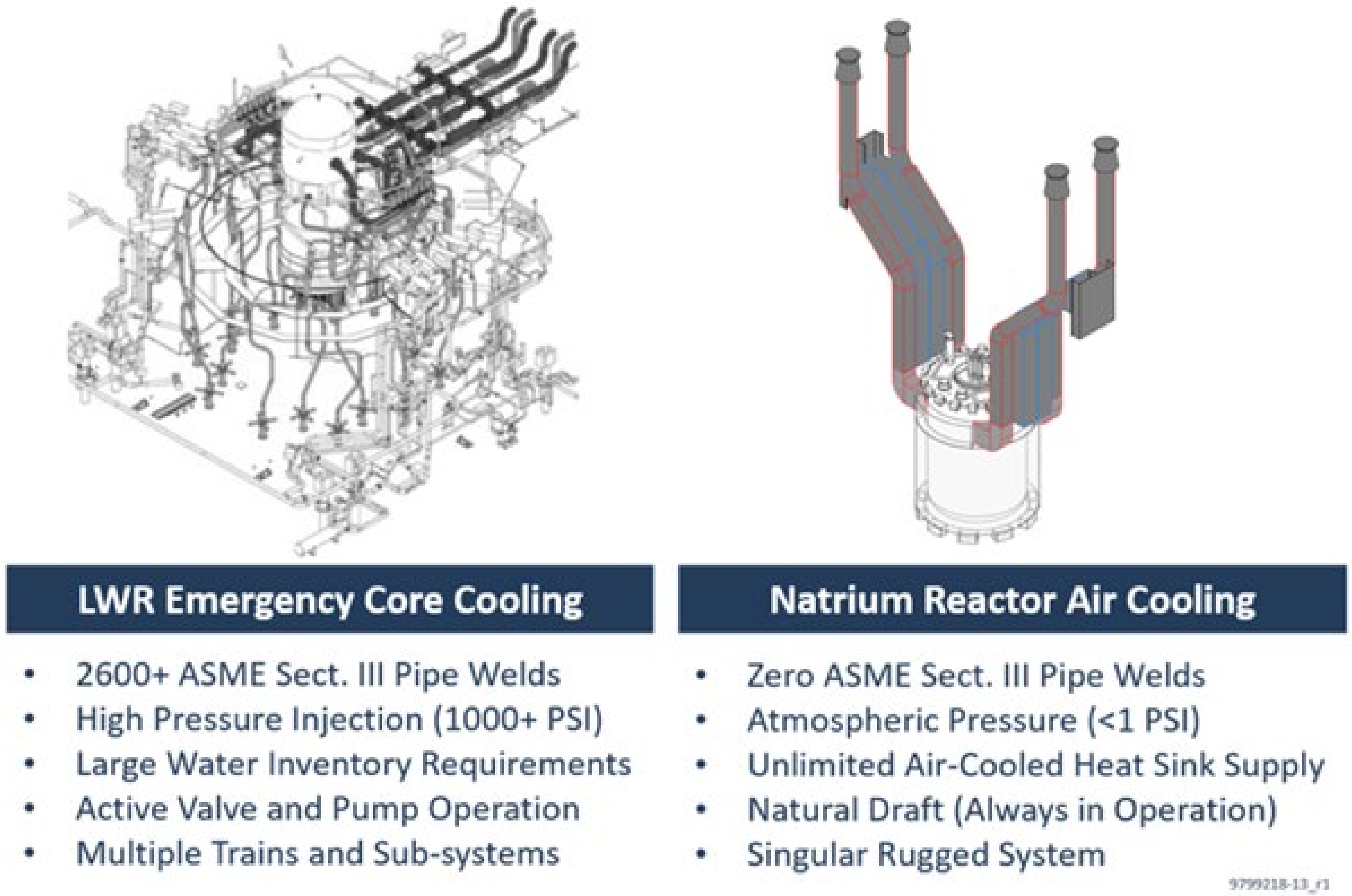
- The simplicity achievable in I&C design is somewhat constrained by the complexity of the overall plant design and its safety approach

- The simplicity of the Natrium plant design and safety approach allow for a simple, small-scope implementation of safety-related I&C functions, compared to past LWR applications

Fuel Cooling – RAC

- Always in operation
- Performs both ECCS and RHR roles
- No automatic or manual control actions to place in service
- No electrical power
- No support systems

Eliminates existence of Safety-Related I&C systems to initiate, control, and monitor ECCS, RHR and EAS equipment



TerraPower NATRIUM

Contain

- No penetrations exist through reactor vessel and guard vessel
- No significant pressure differential across the primary boundary
- Layers of passive barriers and transport inhibitors
- Fail-safe isolation valves on sodium processing and cover gas lines

Eliminates need for I&C to initiate large-scale, active containment isolation functions

Functional Containment: *"A barrier, or set of barriers taken together, that effectively limits the physical transport of radioactive material to the environment"* (SECY-18-0096)

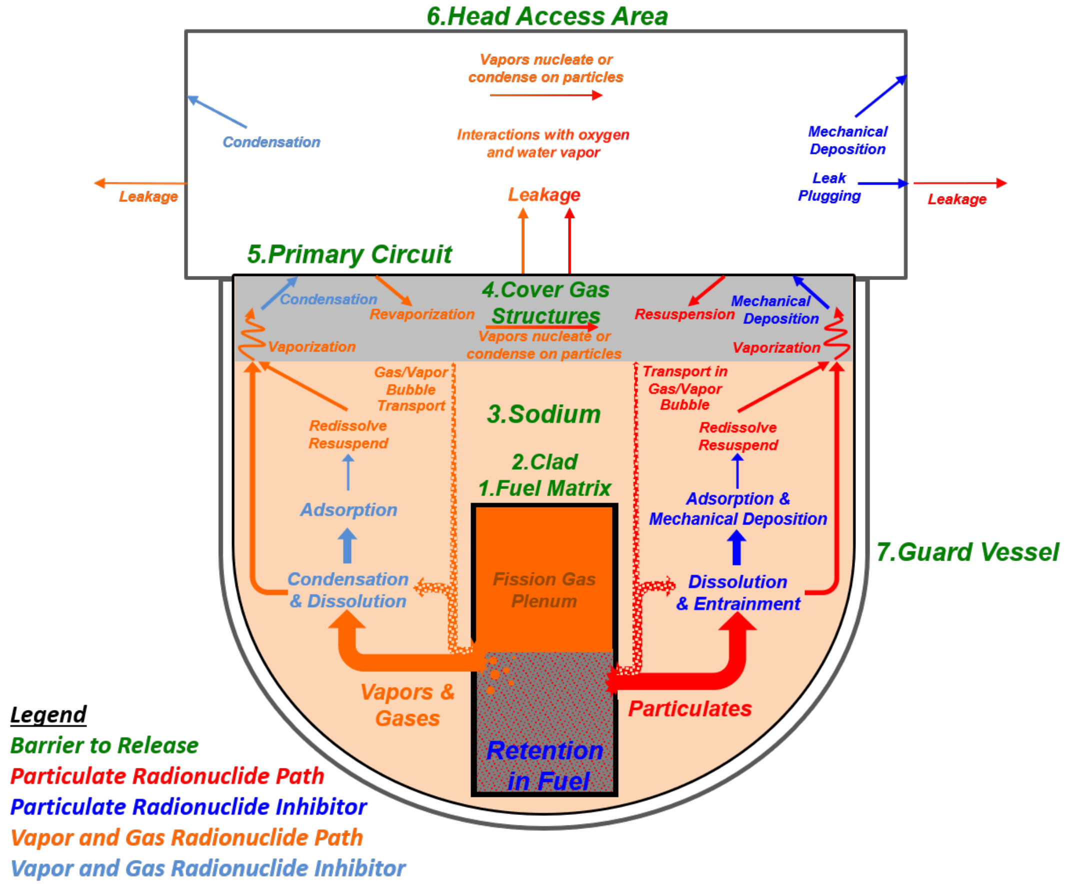


Figure credit: Argonne National Laboratory, ANL-ART-49 Vol 1

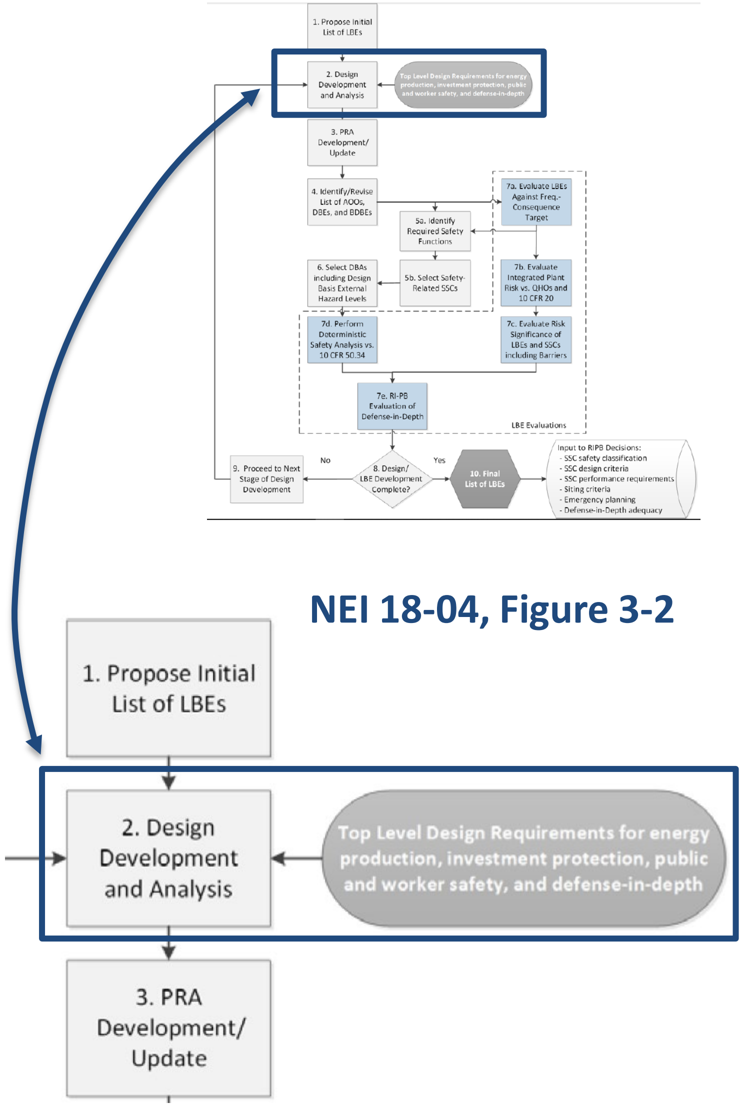
Control of Reactivity – "Scram"

- De-energize to actuate: Removing power from actuation devices frees neutron absorber to fall into reactor core by gravity
- Current design concept: On LOOP, actuation devices are de-energized without requiring action from the RPS.
- Reduced inventory of scram initiating conditions
  – All scram initiations based solely on Nuclear Island parameters
- Molten salt storage tanks eliminate direct coupling of reactor plant and turbine/generator output which is inherent to PWRs and BWRs
  – Decoupling eliminates fast transients in the reactor system caused by BOP failures/maloperation – such failures do not require direct protection by scram

Supports a simple implementation of Safety-Related RPS

Early Design Application of DID

- Design team is applying an explicit Defense Line (DL) approach consistent with IAEA SSR-2/1 DL definitions:
  - Identification of mitigating functions for PIE and event sequences
  - Assignment of functions to DLs
  - Confirmation of two functional DLs capable of mitigating initiating events
  - Derivation 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 exceptional cases, a DL2 function may align with NSRST
- This approach is intended to minimize design iterations and decreases potential for 'surprises' when the RIPB Evaluation of DID Adequacy step is performed



NEI 18-04, Figure 3-2

TerraPower NATRIUM

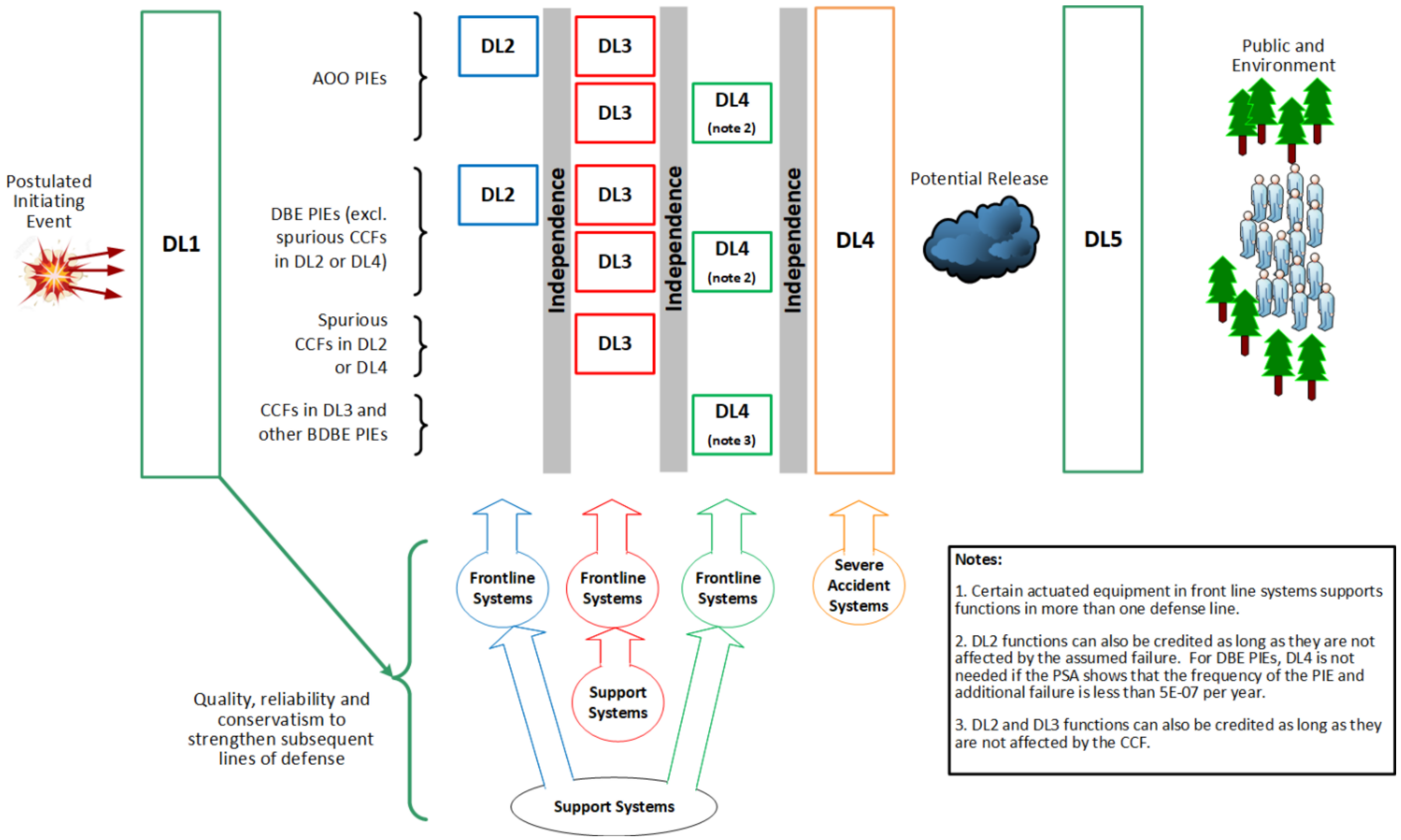
Defense-in-Depth Concept

- **Five DLs** comprising programmatic elements, design features and design functions
- **DL1:**
  - reduce potential for initiating events to occur
  - reduce potential for failures in subsequent DLs
- **DL2, DL3, DL4:**
  - Ensure performance of FSFs in response to initiating events
- **DL5:**
  - Off-site emergency preparedness in case substantial radioactive release occurs or appears imminent

Defense Lines provide a relatively simple, consistent framework to support organizing the design basis

Defense-in-Depth Concept

- Among DLs 2, 3, 4:
  - Two independent lines can mitigate AOO initiating events
  - Two independent lines can mitigate DBE initiating events
  - One line can mitigate DBE initiating event caused by CCF in DL2 or DL4
    - Mitigation means must be independent from effects of initiating CCF
  - Mitigation of initiating event caused by CCF in DL3, and BDBE initiating events, by unaffected functions in any DL



Points of required independence and diversity in I&C Architecture design are determined based on this approach

Defense Line Analyses

- **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

"Event List" is the interface between analysis and design activities, to identify mitigation functions and assign them to DLs.

TerraPower NATRIUM

Event List Example

Seq. ID	Event Sequence Name	PIE	Initiating Fault	DSA Type	Additional Failures	Event Type (Frequency)	Reactivity Control DL Functions	Decay Heat Removal DL Functions	Radionuclide Retention DL Functions	DL1 Design Features
DHS-NSTL-BL	Cold Salt Tank Level Low	Cold Salt Tank Level Low	EI operations error, large component leak, EI trip	Baseline	None	AOO (1/yr to 1E-2/yr)	F9: (**DL2-RC1i**) Power Runback on Low Cold Salt Tank Level, F54: (**DL2-RC5**) CRD Motor Drive-In on Power Runback	F31: (**DL2-HR3a**) Active IAC/AHX Operation on Runback, F55: (**DL2-HR8**) PHT System Flow Control on Power Runback, F56: (**DL2-HR9**) IHT System Flow Control on Power Runback	F37: (DLX-RR1) Inherent - Normal Containment Design Features	DL1-60: The low level setpoint of the Cold Salt Tank shall ensure there is sufficient inventory in the Cold Salt Tank to perform a Power Runback.
DHS-NSTL-CN	Cold Salt Tank Level Low, Power Runback Failure	Cold Salt Tank Level Low	EI operations error, large component leak, EI trip	Conservative	Failure of F9: (DL2-RC1i) Power Runback on Low Cold Salt Tank Level	DBE (1E-2/yr to 1E-4/yr)	F19: (**DL3-RC1b**) Reactor SCRAM on High High Core Outlet Temperature	F33: (**DL3-HR1**) Pump Coastdown, (**DL3-HR4**) Inherent - RAC Operation	F37: (DLX-RR1) Inherent - Normal Containment Design Features	

- Baseline case: full mitigation by DL2 functions
- Conservative case: full mitigation by DL3 functions
- No Extended case required; mitigation by two functional defense lines achieved

I&C Functional Basis

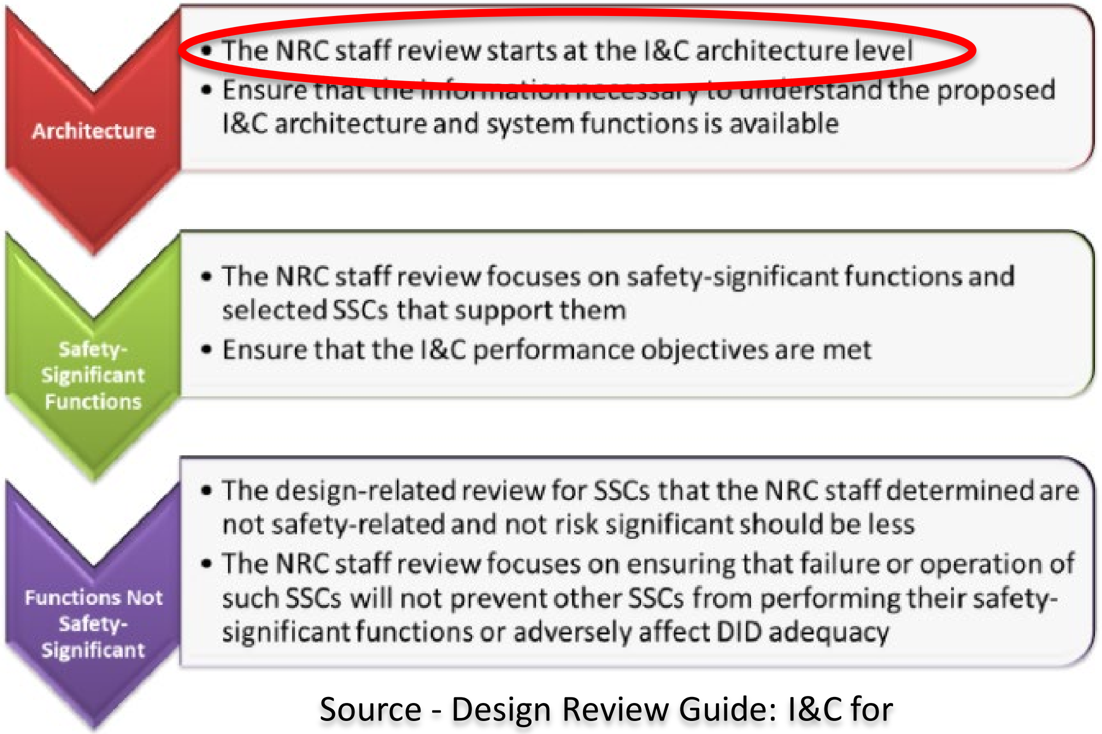
- Plant-level Operational Narratives:
  - Define how the plant is expected to be operated normally
  - Define expected/desired plant responses to off-normal situations
    - The 'off-normal' narratives are currently housed in the Event List sequence summaries
- Plant functions are systematically derived from the Operational Narratives
- Plant functions are decomposed for allocation to plant systems and to I&C Architecture
- I&C Architecture further decomposes for allocation to specific I&C systems

During conceptual design phase, traceability of I&C functions to their originating basis is being established

TerraPower NATRIUM

Plant I&C Architecture - Basics

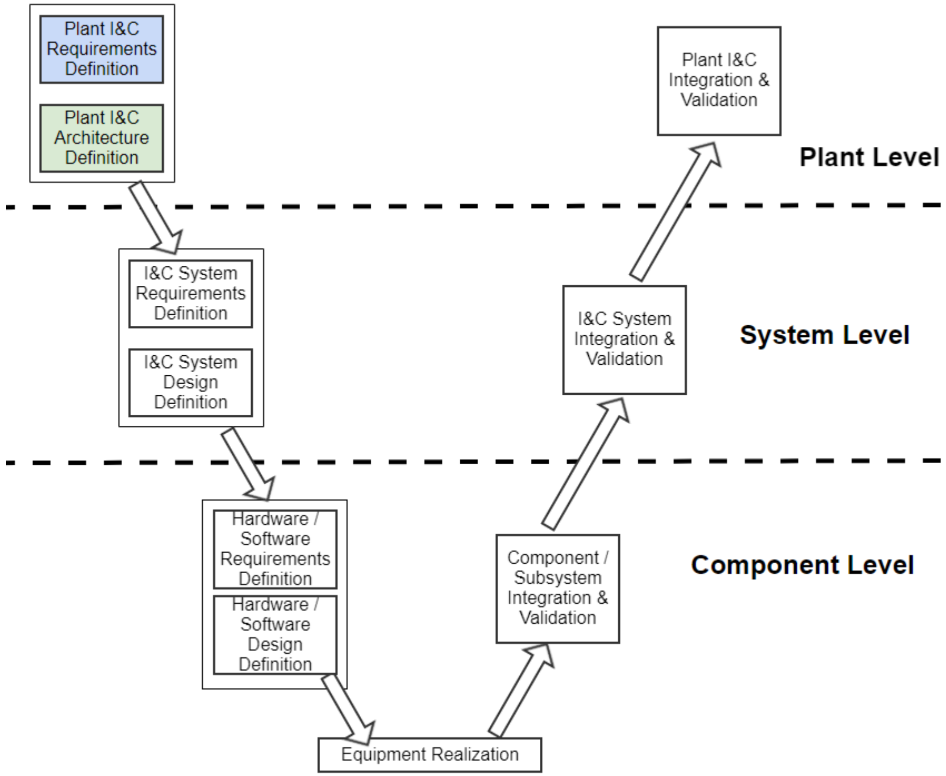
- The Plant I&C Architecture is the *organizational structure* of the I&C systems in the plant
- Organizational structure comprises definition of each I&C system in terms of its:
  - Assigned functions
  - Safety classifications, and
  - Relationships to other systems (including communication between I&C systems)
- The Plant I&C Architecture design is where the I&C implementation of the Defense-in-Depth Concept can be most readily defined and understood;
- 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 - Design Review Guide: I&C for non-LWR Reviews

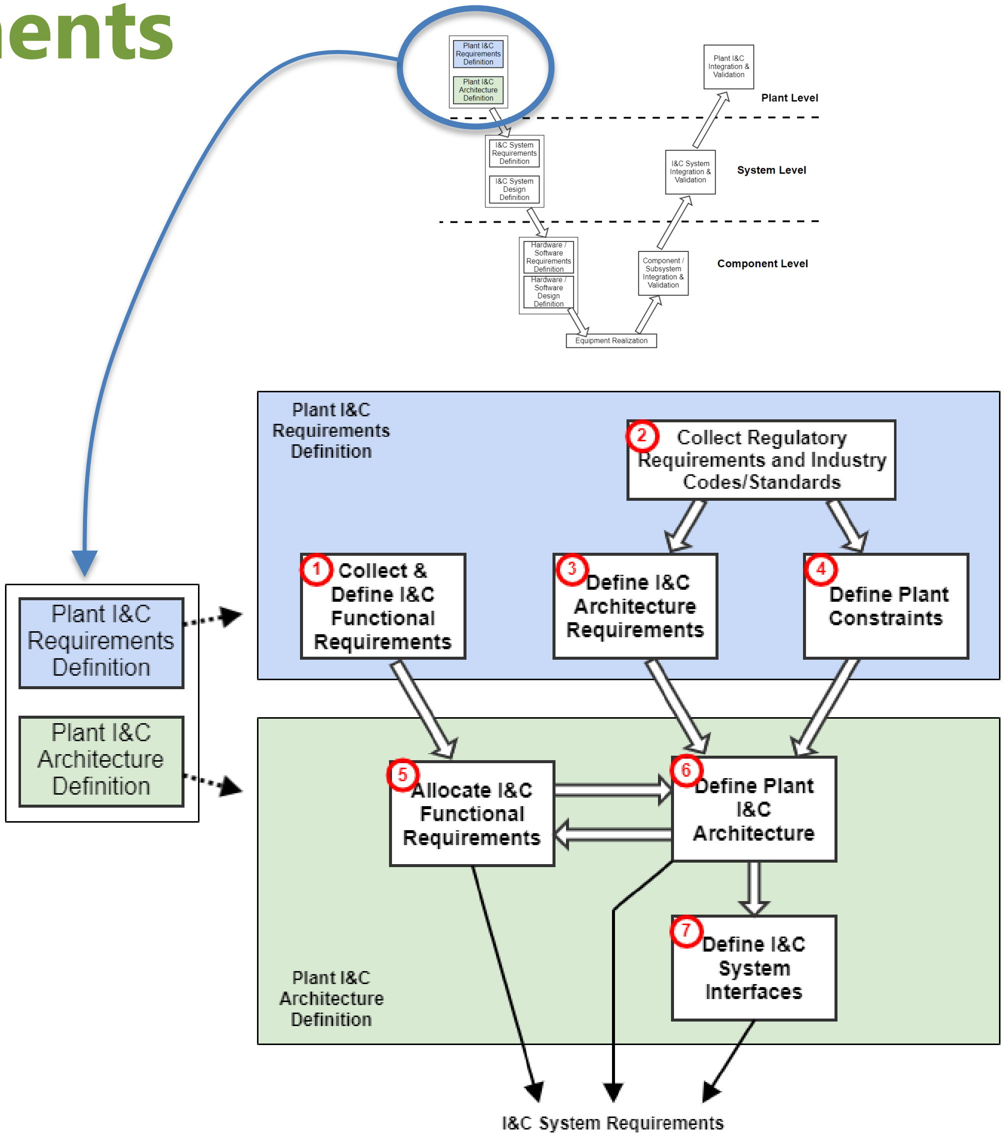
Plant I&C Architecture - Process

- Plant-Level I&C Architecture translates plant-level functions, performance objectives, and constraints into I&C system requirements
- I&C Architecture Design Plan used to 'control' the design activities in the Plant I&C Architecture scope
- Current focus is on initial requirements definition and architecture design
- Future activities
  - Coordination and architecture updates to reflect I&C system design progression and plant design progression
  - Plant-level I&C integration and validation



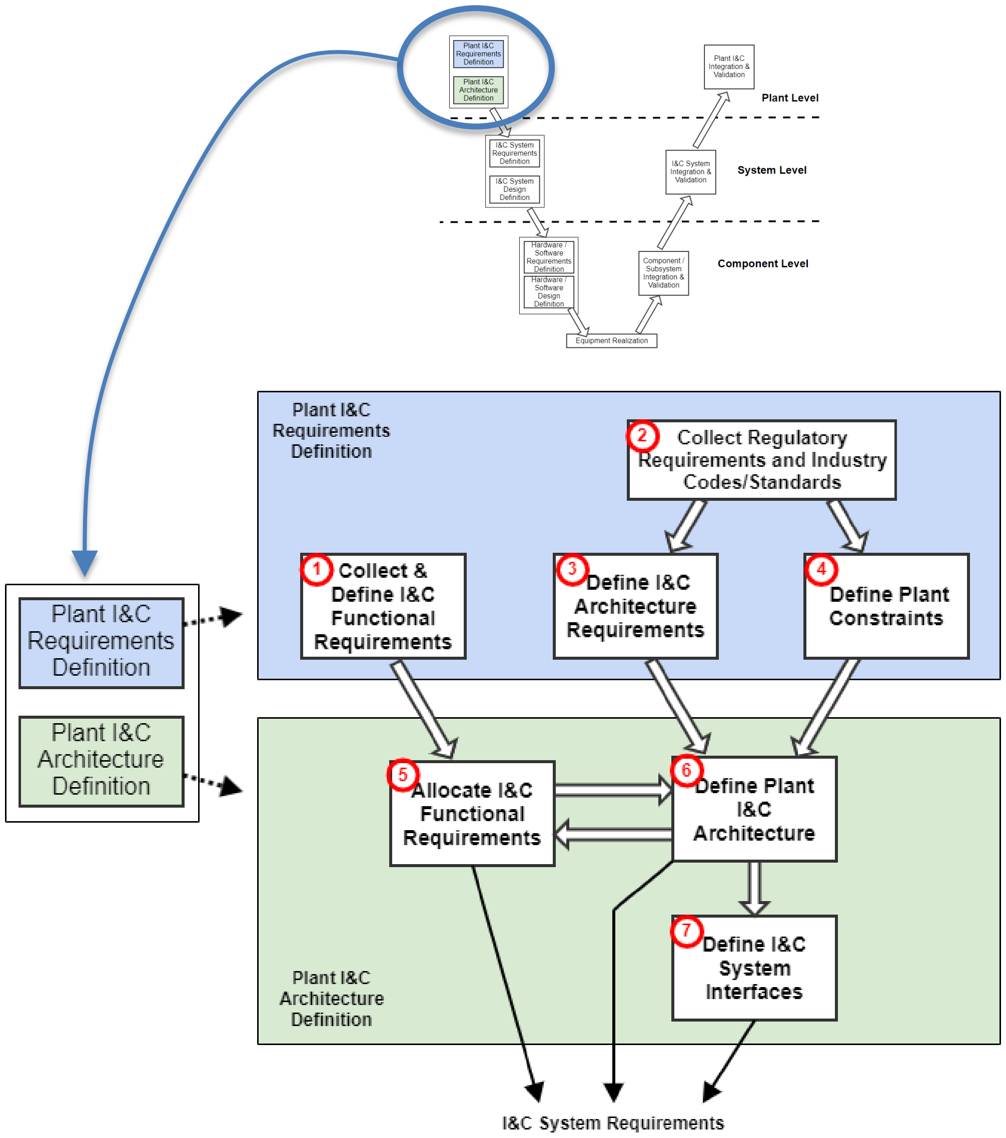
Plant I&C Architecture - Requirements

1. Collect and define I&C Functional Requirements
   – Define the necessary functions to control, operate and/or monitor a defined part of the plant process
2. Collect regulatory requirements, codes and standards
   – Identify those that are applicable, scope of applicability and derivation of project/design-specific requirements to implement
3. Define I&C 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. Define Plant Constraints
   – Identify constraints placed on the I&C from 'external' influences, such as: Plant building and room layouts, environmental conditions, human factors, cyber security, process system interfaces, on-line maintenance approaches, etc.



Plant I&C Architecture - Design

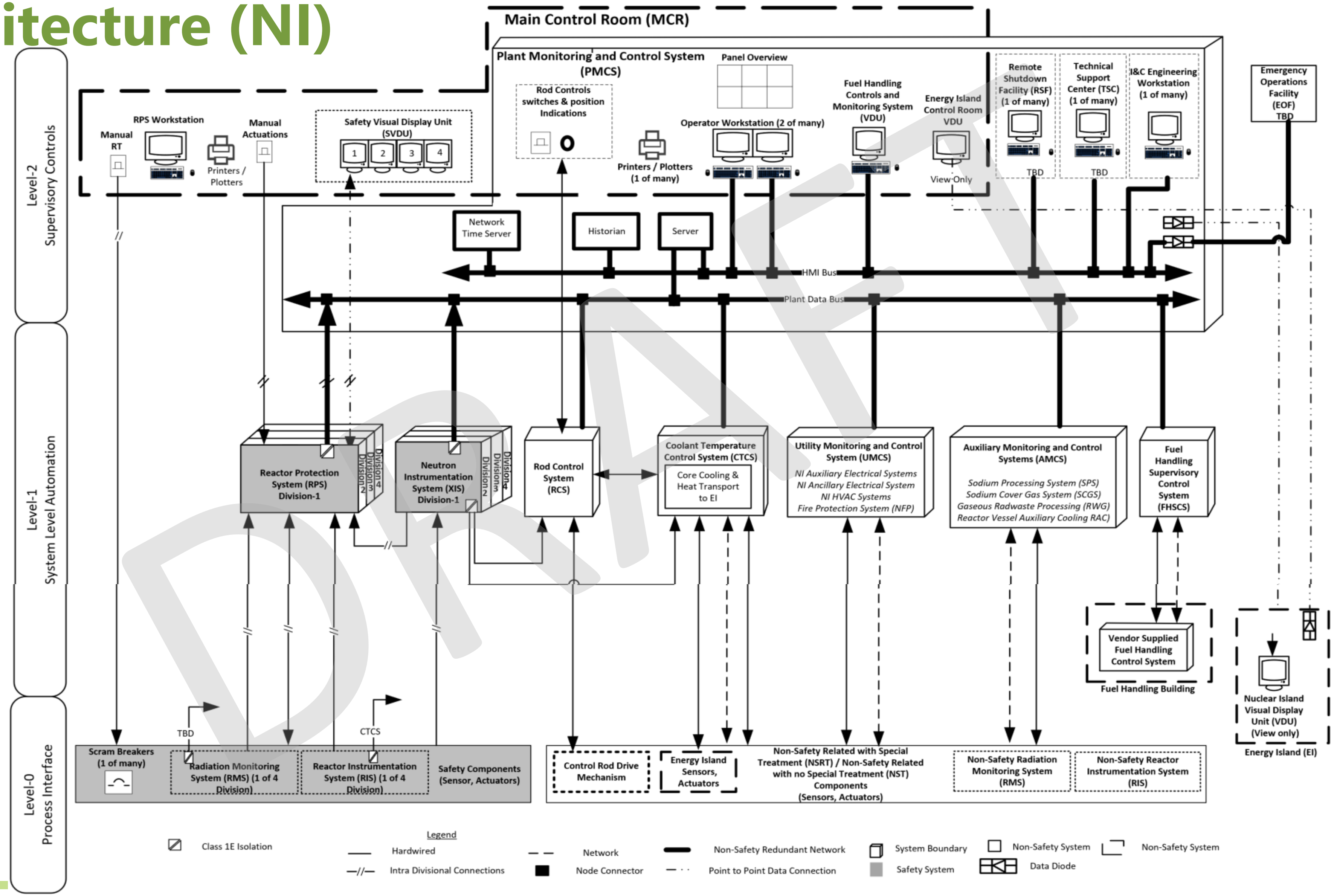
5. Allocate I&C Functional Requirements
   - Establish criteria to govern the process of decomposing I&C functions and allocating to I&C systems
   - The act of function allocation establishes the justification for existence of interfaces between I&C systems
6. Define Plant I&C Architecture
   - Establish the definition of each I&C system including its:
     - Design basis functions
     - Position among the Defense Lines
     - Safety Classification
     - Implementing technologies (technology platform)
     - Necessary interfaces
     - Physical location in the plant
7. Define I&C Interfaces
   - Establish specific requirements to govern implementation of interfaces between I&C systems



TerraPower NATRIUM

Conceptual I&C Architecture (NI)

Figure : Nuclear Island I&C Architecture Diagram for Natrium



TerraPower NATRIUM

DRG: I&C for Non-LWR Reviews

- Key messages from the DRG:
  - Increased focus on how I&C supports plant-level objectives:

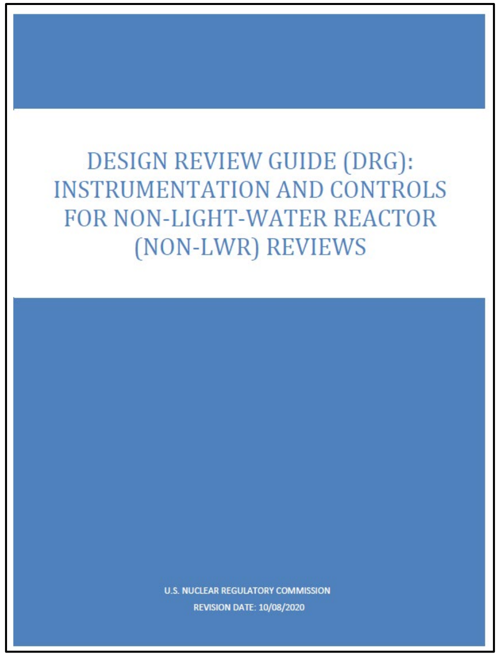
> *"The reviewer should focus on verifying the applicable attributes of the I&C system design that support the plant level performance objectives…*

  - Acknowledgement of importance of plant-level I&C Architecture:

> *"…implementation of the DID concept for I&C is achieved mostly at the I&C architectural level by allocating I&C functions into systems belonging to different levels of defense within the I&C architecture"*

  - Recognition that diversity is in support of DID; not a goal in-and-of itself:

> *"While diversity is part of the fundamental I&C design principals, it is only considered as one means to address CCF. Therefore, the review guidance focuses more broadly on the diversity in support of DID assessment"*


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

U.S. NUCLEAR REGULATORY COMMISSION
REVISION DATE: 10/08/2020

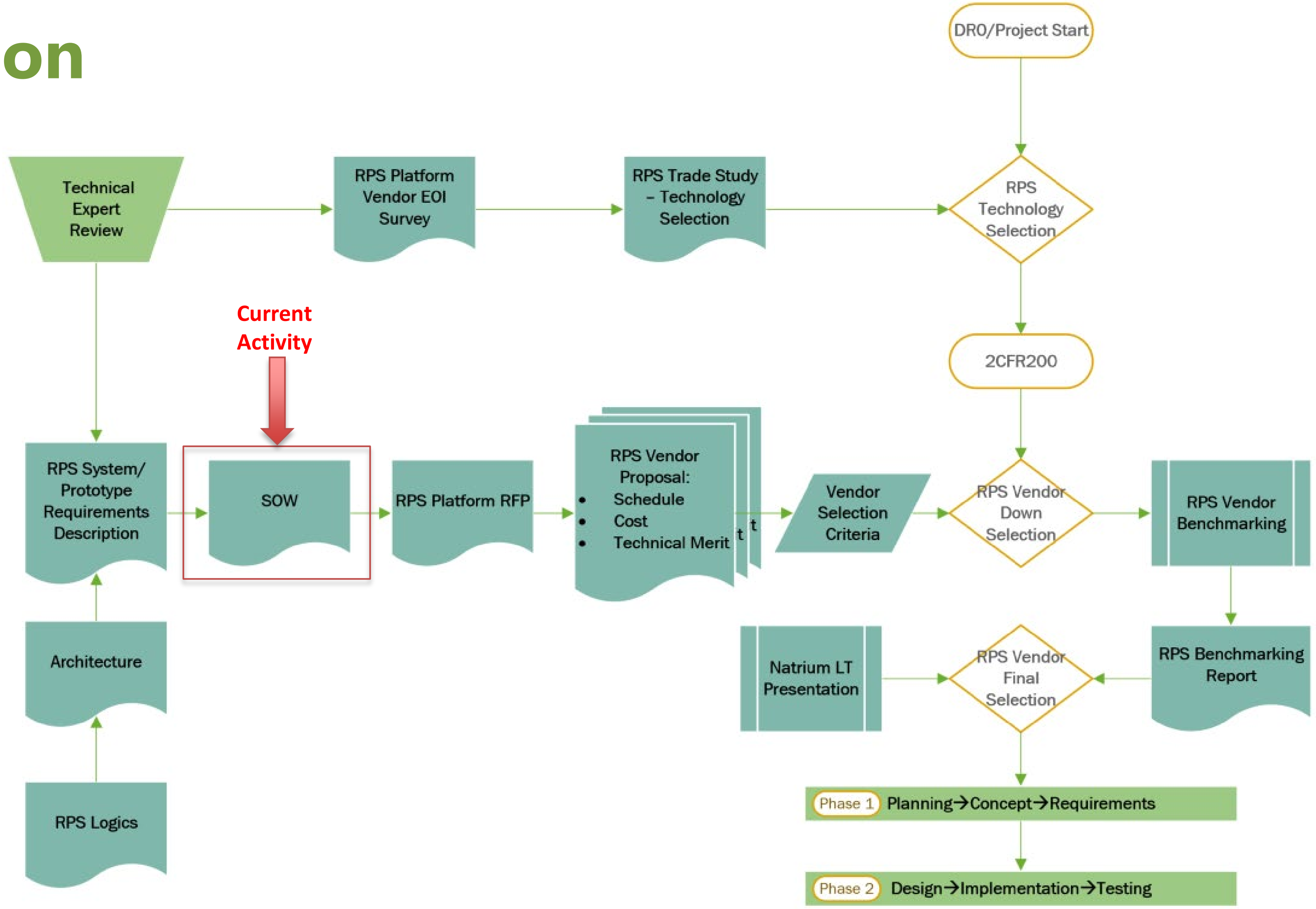
TerraPower NATRIUM

DRG: Topics for Future Engagements

- Systematic Assessment
- Safety Demonstration
- I&C Hazard Analysis
- App. A relationship to existing review guidance
- Codes/Standards selection; e.g., IEEE vs. IEC

RPS Vendor Selection

- Establishing early partnership with RPS platform vendor is a priority
- Rigorous technology/vendor selection process established
- In preparation for RFP, Statement of Work currently under development



TerraPower. NATRIUM

Vendor Selection Criteria

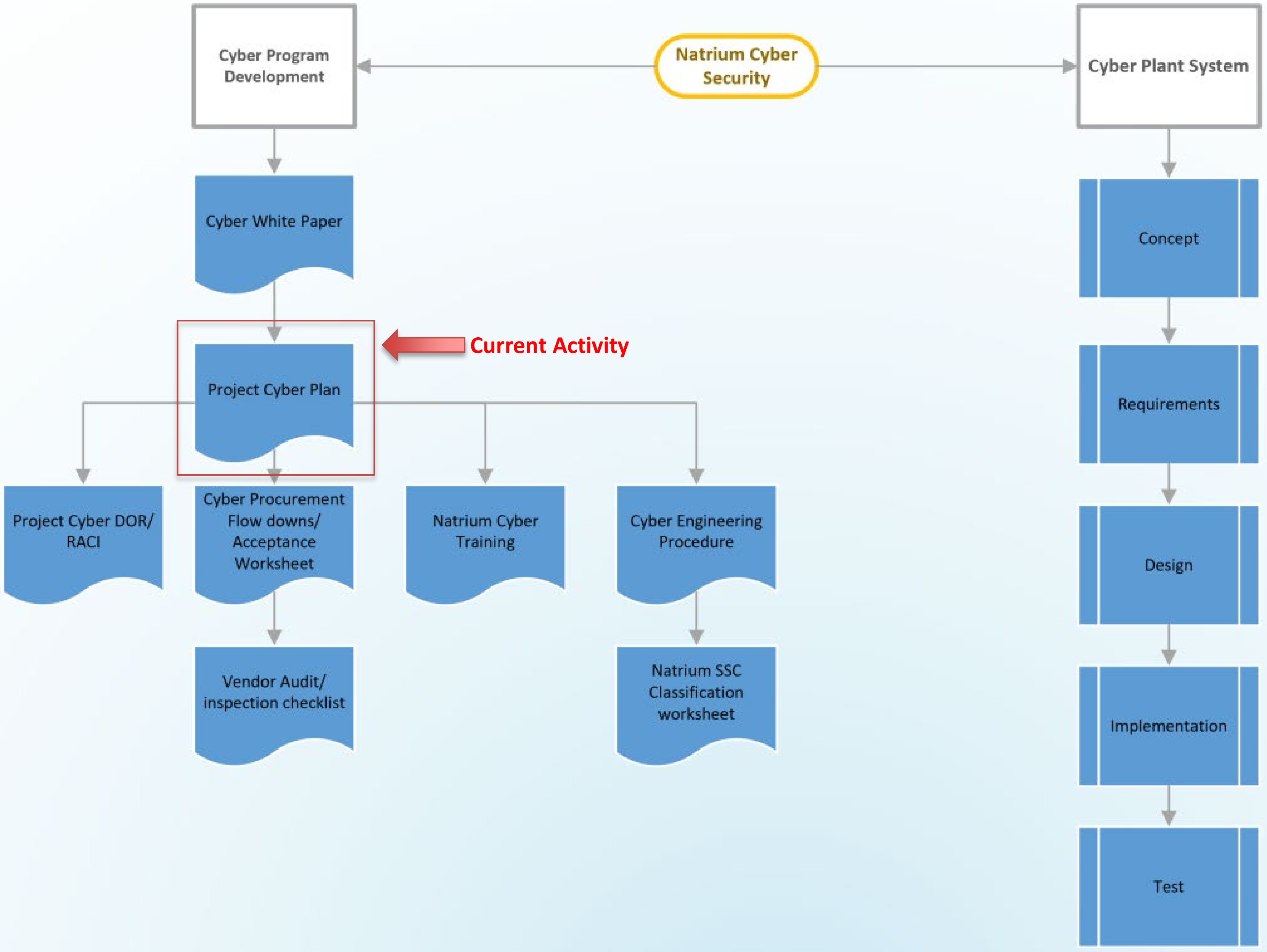
General	III – Quality
Responsiveness to RFP – Bidders must submit all proposal forms	Quality Program - 10 CFR Part 50, appendix B
Document quality – references, support for claims	NRC Regulations Title 10, Code of Federal Regulations Part 21
On-time submittal	Cyber programs including SDOE, supply chain, etc are in compliance with industry best practice
I - Management & Operations	IV - Regulatory Acceptance
Feedback from previous customers	Regulatory project fit/licensing risk
Management and technical staff defined and adequate	Diversity/common cause failure - No DAS Required
Supply chain reliability and quality	V - Business & Contract
Resource commitments identified and adequate	Total Cost - must be reasonable and supported
II – Technical	Schedule accuracy and time to Market including supply chain reliability
Technology Readiness and Maturity	Cost allocation between elements is well defined and supported
System characteristics including performance, footprint, fit and finish	Contract - acceptance of terms and conditions
Maintenance, support, training	Assignment of IP
Prototype, simulator, modeling, or emulation of RPS system.	Country of origin for components
Reliability determined by PFD	
Source code/ models for site-specific and platform provided	

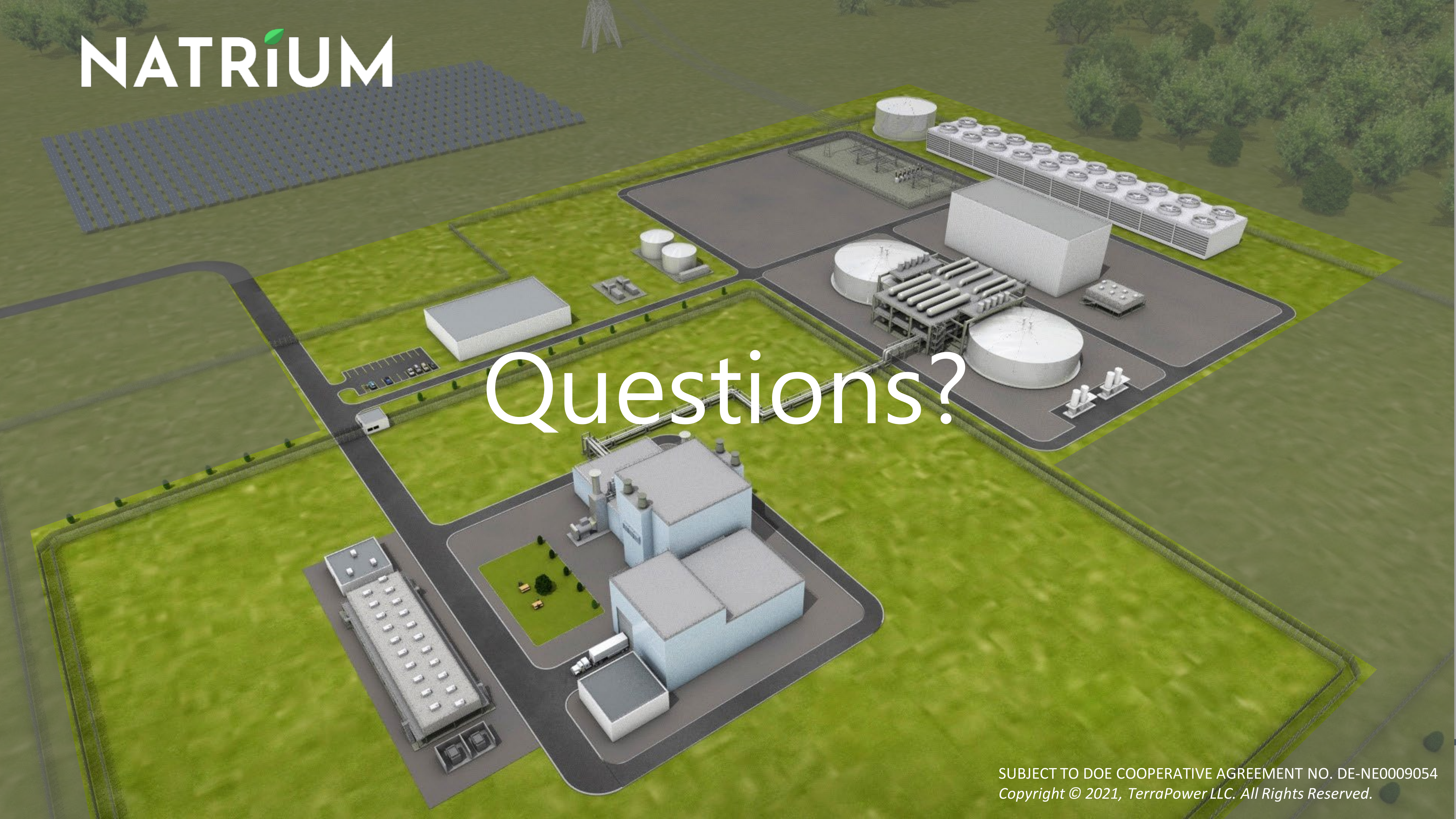
RPS Vendor Selection Considerations

- Analog vs. Digital (PLC vs. FPGA)
- Intellectual property assignment (per 2 CFR 200; long term RPS maintenance)
- Codes and Standards – Which version/revision to specify
  – E.g., 2004 vs. 2016 version of IEEE-1012

Cyber Security

- Cyber security must be integrated from conceptual design through operation of the facility
- Both programmatic efforts and plant system development efforts and included
- Standardized flow down to vendors and subcontractors (supply chain) to assure consistent cyber treatment
- Cyber Security Plan under development





Questions?

SUBJECT TO DOE COOPERATIVE AGREEMENT NO. DE-NE0009054

Acronym List

AC - Alternating Current
AOO - Anticipated Operational Occurrence
ARDP – Advanced Reactor Demonstration Program
BDBE - Beyond Design Basis Event
BOP - Balance of Plant
BWR - Boiling Water Reactor
CCF - Common Cause Failure
CFR – Code of Federal Regulations
DBE - Design Basis Event
DID – Defense-in-Depth
DL - Defense Line
DRG - Design Review Guide
EAS - Essential Auxiliary Support
EBR – Experimental Breeder Reactor
ECCS - Emergency Core Cooling System
FFTF – Fast Flux Test Facility
FPGA - Field Programmable Gate Array

HX - Heat Exchanger
I&C - Instrumentation and Control
LBE – Licensing Basis Event
LMP – Licensing Modernization Project
LWR - Light Water Reactor
PIE - Postulated Initiating Event
PLC - Programmable Logic Controller
PSAR – Preliminary Safety Analysis Report
PWR - Pressurized Water Reactor
QA - Quality Assurance
RFP - Request for Proposal
RHR - Residual Heat Removal
RIPB – Risk-Informed, Performance-Based
RPS - Reactor Protection System
SFR – Sodium Fast Reactor
SRP - Standard Review Plan
TREAT – Transient Reactor Test