Enclosure 5
Design Approach for Diversity & Defense-in-Depth Slides
(Redacted)

generation

mPower

Design Approach for Diversity & Defense-in-Depth

December 10, 2013

(Redacted Version)

This material is based upon work supported by the Department of Energy under Award Number DE-NE0000583.

This is a pre-application document and includes preliminary B&W mPower™ Reactor design or design supporting information and is subject to further internal review, revision, or verification.

generation mPower

Meeting Objectives

- Review and Summarize Information from August 28, 2013 meeting with NRC Staff
- Provide NRC staff with an update to mPower I&C design approach as it applies to Diversity and Defense-in-Depth
- Provide follow-up to issues raised at Aug 28, 2013 Meeting
- Discuss path forward toward completion of DCD Ch. 7

generation mPower

Agenda

- Introductions
- Review of Material from Previous Meeting with NRC Staff on August 28, 2013
- Review mPower Approach to Diversity and Defense-in-Depth (D3)
- Review Diversity Concepts
- Proposed NRC Interaction Schedule & Topics

generation mPower

Review of Information Presented Previously to NRC Staff at August 28, 2013 Meeting

mPower Approach to Meet DSRS Chapter 7 Guidance

- DSRS Section 7.1.5 – Diversity and Defense-in-Depth (D3)
  - Continuing evaluation [

    ]

  - Scope of D3 analysis to be limited to [

    ]

Review from Aug. 28 presentation

[Proprietary per Affidavit 4(a)-(f)]

generation mPower

Echelons of Defense in Depth

[

]

[Proprietary per Affidavit 4(a)-(f)]

generation mPower

I&C System Architecture

- I&C Architecture supports inherent diversity strategy for all AOOs/PAs
  - [

    ] *(This is changed)*
  - [

    ] (*no change*)
- Aspects of simplicity incorporated in architecture design:
  - No unnecessary or non-essential features *(no change)*
  - RT and ESF algorithms kept as simple as practicable *(no change)*

Review from Aug. 28 presentation

[Proprietary per Affidavit 4(a)-(f)]

generation mPower

Review of I&C Safety System Design Technology

- Safety I&C System Technology Selected

  ]

- Basis for Selection

  [

  ]

  - Key factors → Simplicity, Licensability, Predictable/Repeatable Behavior, Testability

- Continued evaluation of technology options to minimize/eliminate need for diverse actuation system

Review from Aug. 28 presentation

No runtime software coupled with extremely high level of testability…. Virtually eliminates potential for failures related to software errors

generation mPower

Review: mPower Approach to Inherent Diversity

- Two groups of safety RTS/ESF functions ***per division*** *(this has changed)*
- Perform diversity analysis to confirm:
  - Primary/Backup protection for AOOs/PAs…Minimize probability and consequence of credible safety-related system CCFs to acceptable levels.
  - Anticipate acceptable consequences → **[ ]**

Diversity Attribute (NUREG-CR/6303)	Selectable Options for Design Requirements
Design Diversity	Different approach and technology (e.g., flash-based FPGA and anti-fuse FPGA), each with its own separate set of development tools
Equipment Diversity	Different manufacturers of different designs
Functional Diversity	Multiple layers of systems for mitigation of plant transients
Human Diversity	Different design/implementation teams, same V&V team
Signal Diversity	DNB protection from low RCS pressure OR loss of forced circulation
Software Diversity	Different fundamental logic & algorithm structure

Review from Aug. 28 presentation

[Proprietary per Affidavit 4(a)-(f)]

generation mPower

Review: APS Block Diagram from August, 2013

Review from Aug. 28 presentation

[

]

[Proprietary per Affidavit 4(a)-(f)]

generation mPower

Conclusions from August 28, 2013 Meeting

- D3 Design Conforms to Current DSRS Guidance
- D3 Technical Report planned for 2Q2014

generation mPower

Follow-up to Issues at August 28, 2013 Meeting

- Use of Inherent Diversity…Primary functions evaluated as part of Chapter 15 Safety Analysis, Backup functions evaluated using "best estimate" methods.
- Algorithms diversified [
  ]
- How will diversity be addressed in the V&V process?
  - Same Independent (from design team) V&V team across entire platform
- How does inherent diversity manifest itself in the architecture [ ]

generation mPower

I&C System Architecture

[

PRELIMINARY

]

[Proprietary per Affidavit 4(a)-(f)]

generation mPower

Current Diversity Concepts and I&C System Architecture

generation mPower

Architectural Diversity Options

- 3 Main Concepts Considered for Inherent Diversity within RTS/ESF to Mitigate CCF [

]

[Proprietary per Affidavit 4(a)-(f)]

generation mPower

Concept A

[

PRELIMINARY

]

[Proprietary per Affidavit 4(a)-(f)]

generation mPower

Concept B

[

]

generation mPower

Concept C

[

PRELIMINARY

]

[Proprietary per Affidavit 4(a)-(f)]

generation mPower

Concept Selection Summary

[

]

[Proprietary per Affidavit 4(a)-(f)]

mPower APS Diversity Specifics

- Design Diversity
  - Different approaches within a technology
- Equipment Manufacturer Diversity
  - Different manufacturers of fundamentally different equipment designs
- Logic Processing Equipment Diversity
  - Different logic processing equipment architectures
- Functional Diversity
  - Different purpose, function, control logic, or actuation means of same mechanism

mPower APS Diversity Specifics (Cont.)

- Life Cycle (Human) Diversity
  - Different design organizations (possibly within same company)
  - Different designers, engineers, and/or programmers
  - Different testers, installers, or certification personnel
- Signal Diversity
  - Different reactor or process parameters sensed by different physical effects
  - Different reactor or process parameters sensed by the same physical effect
  - Same process parameter sensed by different redundant set of similar sensors
- Logic (Software) Diversity
  - Different algorithms, logic, and logic architecture
  - Different timing or order of execution
  - Different runtime environments (i.e., no runtime software)
  - Different functional representations? (Possible, but not credited)

generation mPower

Functional and Signal Diversity Specific Concepts

generation mPower

Functional Diversity – from NUREG/CR-6303

- Different underlying mechanism
  - RTS: Reduce reactor power – rod insertion by gravity, rod insertion by motor driving, strong negative moderator coefficient , boron injection tank
  - ESFAS: Commence emergency cooling – 2 trains of ECC automatic depressurization
  - ESFAS: Commence isolation – 2 isolation valves for FW and STM based on BOP parameters; containment isolation based on CNT and RCS parameters
- Different function, purpose, control logic, or actuation means
  - RCS Thot/Tavg control to maintain LCOs with rod control
  - Pressure control to maintain LCOs with spray and heaters
  - Water level control to maintain LCOs with RCI inventory management and inherent level changes due to water specific volume changes
- Different response times
  - Loop transport times and water inventories establish how plant responds
  - Time to boil off OTSG gives time before RCS heats up significantly

generation mPower

Diversity of Instrument Signals for RTS and ESFAS Functions

[

PRELIMINARY

]

[Proprietary per Affidavit 4(a)-(f)]

generation mPower

Signal Trip Function Allocation for Overall AOO/PA Diversity

Trip Function	Increase in Heat Removal	Decrease in Heat Removal	Decrease in RCS Flow	Reactivity and Power Distribution Anomalies	Increase in RCS Inventory	Decrease in RCS Inventory
High Power Range Neutron Flux (Low Power Setting) **(S3)**	15.1 (B)			15.4.1 (B, slow)		
High Power Range Neutron Flux (High Power Setting) **(S1)**	**15.1 (P)**			**15.4.2 (P, fast)**		
Low RCP Speed **(S1)**			**15.3 (P)**			
Low PZR Pressure **(S1)**	15.1 (B)			**15.4.3 (P, drop)**		**15.6 (P, fast)**
Variable Low Pressure Temperature **(S1)**	15.1 (B)			**15.4.3 (P, drop)**		**15.6 (P, fast)**
High PZR Pressure **(S1)**		**15.2 (P)**	15.3 (B)	15.4.2 (B, slow)	**15.5.2 (P, fast)**	
High Containment Pressure **(S1)**	**15.1.5 (P, HELB)**					15.6 (B)
Low IEOTSG Water Level (Low Power ESFAS) (S2)	15.1.5 (B)	15.2.7-8 (B)				
High Intermediate Range Neutron Startup Rate **(S1)**	15.1 (B)			**15.4.1 (P, fast)**		
High Intermediate Range Neutron Flux (Low Power Setting) **(S1)**	15.1 (B)			**15.4.1 (P, slow)**		
High RCS Temperature (T_{HOT}) **(S1)**		15.2 (B)		15.4.2 (B, slow)		
Low RCS Flow **(S2)**			**15.3 (P)**			
Low PZR Water Level **(S2)**	15.1 (B)					**15.6 (P, slow)**
High PZR Water Level **(S2)**		15.2 (B)		15.4.2 (B, slow)	**15.5.2 (P,slow)**	
Low Feedwater Flow **(S2)**		**15.2.7 (P)**				
Low STM Pressure (HELB, IO-RV) **(S1)**	**15.1.5 (P, HELB)**	15.2.8 (B)				

(P) – Primary **(B)** – Backup
HELB – High Energy Line Break
IEOTSG – Integral Economizer Once Through Steam Generator
Slow, fast – rates of change in AOO systems response
drop – control rod drop
IO-RV – Inadvertent Opening of Relief Valve

(NUREG/CR-6303 Section 3.2.5 Signal Diversity Definitions
(S1) – Reactor parameters by sensed different physical effects
(S2)– Different parameters sensed by same physical effect
(S3)– Same parameters sensed by redundant set of sensor

generation mPower

Operating Conditions at Power

[

]

[Proprietary per Affidavit 4(a)-(f)]

generation mPower

ESFAS Functions

Action	Process Parameter Signal	PA or AOO Mitigated
Isolate Containment	High Containment Pressure	LOCAL, HELB in CNT
Isolate Steam and FW	Low Steam Pressure Low FW Flow Low OTSG Water Level	HELB Complete loss of FW
Open High Pressure ADV	High PZR Pressure	Loss of Heat Removal
Isolate RCI Letdown	Low PZR Water Level (RT level)	Reduction in Inventory LOCA
Open High Pressure ADV	Low PZR Water Level when PZR Pressure [ ]	Small, High Break LOCA Reduction in Inventory
Open Low Pressure ADV	Low PZR Pressure	Establish RWST flow for ECC after IPIT tank flow
Trip RCPs OFF	Signal to OPEN HP/LP ADVs	No specific mitigation function

generation mPower

Signal Diversity…In Summary

- Goal for Inherent Diversity…Focus on high diversity within RTS and ESFAS to cover the spectrum of all the AOOs and PAs
  - Sufficient Diversity for a Broad Range of AOOs/PAs
  - Sufficient "Coverage" within an Event Type with:
    - the primary credited trip function with 2 out of 4 sensors
    - potential set of backup sensors & functions that could mitigate the event in the D3 coping analysis
    - depends on how one considers the fault of the RTS for CCF conditions

[ ]

generation mPower

Proposed Future NRC Interaction Schedule

- Proposed monthly Interaction with the NRC:
  - February 2014 – Hazards Analysis Plan Outline, DCD Chapter 7 content; DSRS implementation
  - April 2014 – Chapter 7 Readiness Review
  - 2Q2014 – D3 Technical Report

generation mPower

Questions?