

**Attachment 3  
I&C Meeting Slides (Redacted)**

generation

---

***mPower***

*B&W mPower™ I&C Design Architecture Update*

*May 16, 2012*

- B&W mPower I&C Architecture Overview
- Applicable NRC Regulations
- Systems Engineering Application to I&C Design
- B&W mPower Control System Architecture
- Fundamental Design Principles
- B&W mPower Control System Manual Operations
- Trips and Operational Bypasses
- Priority Logic Concepts
- Next Steps
- Definitions Glossary

# **B&W mPower I&C Architecture Overview**

- Highly-Reliable, Integrated and Scalable Digital I&C System
- I&C System Must Have Highest Degree of Licensing Certainty
  - Complies with Regulatory, URD Requirements
  - Minimizes Regulatory Challenges with Digital I&C...Cyber-security, Diversity, Independence
- Integrated, Modernized Human-Factored Design
- High-level of Plant Automation
  - Control of Startup, Shutdown, Load Following...support staffing plan
- Deliver Comprehensive O&M Strategy
  - Use of commercially-available components
  - Managed obsolescence

# Key Design Attributes of mPower I&C System

---

[

]

- **Diverse Actuation System (DAS)**

[CCI per Affidavit 4(a)-(d)]

- [ ] [CCI per Affidavit 4(a)-(d)]  
• Analysis to determine shared or separate sensors for DAS

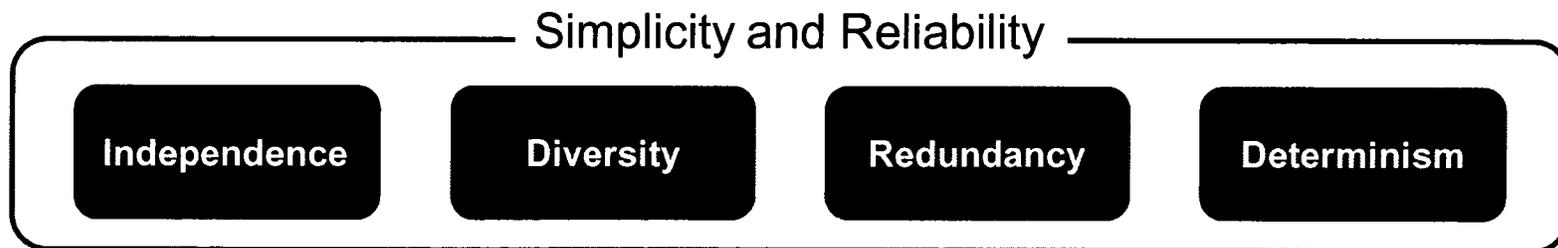
- [ ] coincidence

[CCI per Affidavit 4(a)-(d)]

# mPower Control System (mPCS) Development Process

---

- Classical systems engineering approach ensures that the mPCS will meet two fundamental directives:
  - NRC Requirements
  - B&W Internal Requirements
- Main Focus on defining basic system architecture, interactions, and hazards analysis.

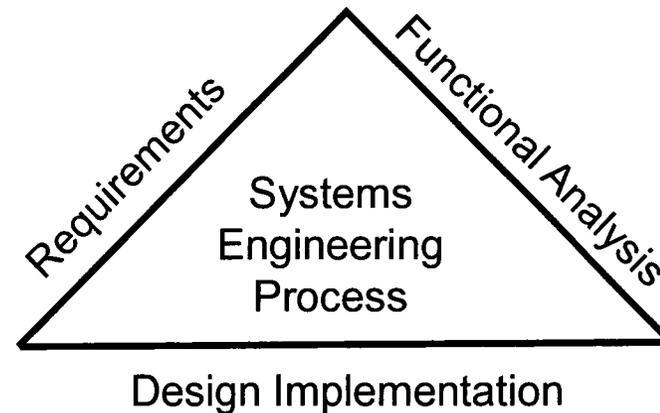


# Applicable NRC Regulations

- The five key sources of authoritative requirements to use as regulatory basis:
  - 10 CFR 50, 10 CFR 52
  - 10 CFR 73.54
  - IEEE 603-1991
  - IEEE 7-4.3.2
- Other relevant documents will be referenced when derived requirements are related to the source document.
  - Regulatory Guides
  - Interim Staff Guidance
  - Branch Technical Positions
  - Industry Standards

# **Systems Engineering Application to I&C Design**

- mPCS is being developed through a rigorous systems engineering process:
  - › Functional Analysis
  - › Requirements Development
  - › Design Implementation



# Classical Systems Engineering “V”

---

- The classic system engineering “V” guides the process
- Going down the left side, requirements, in increasing detail, down to the smallest assembly
- Going up the right side, testing, in decreasing detail, up to the top assembly
- Horizontal Lines indicate verification of requirements for a given level

[

]

[CCI per Affidavit 4(a)-(d)]

- Functional Analysis Determines what the system needs to do
- Provides graphical depiction of what is needed and how assemblies relate to each other
- Functional Analysis is an organized, intuitive vehicle for developing requirements
  - Use cases and activity diagrams are aspects of functional analysis used in this phase

Functional Analysis ensures simplicity in design  
Avoids over complexity, assigns singular functional requirements to sub-systems and components

# mPCS Level Use Case Example

---

[

]  
[CCI per Affidavit 4(a)-(d)]

# Activity Diagram—Increase in Heat Removal

---

[

]

# Storing and Managing Requirements

---

- Requirements stored in DOORS requirements database
  - More organized and manageable than Word document
  - Requirements for a system or assembly stored in Modules, also called requirement specifications

[

]

[

]

[CCI per Affidavit 4(a)-(d)]

# B&W mPower Control System Architecture

# mPCS Architecture – Top Level Block Diagram

---

[

]

# Integrated Top Level I&C Architecture Overview

---

[

]

# I&C System Allocation for Standard 2-Unit Plant

---

[

]

[CCI per Affidavit 4(a)-(d)]

[

]

[

]

[

]

[CCI per Affidavit 4(a)-(d)]

[

]

[

]

# Block Diagram for APS Div III and DAS Div III

---

[

]

[CCI per Affidavit 4(a)-(d)]

# Fundamental Design Principles

# Application of Fundamental Design Principles: Independence

---

[

]

[CCI per Affidavit 4(a)-(d)]

Provisions for Manual Actions in event of Failure of Automatic Function

# Application of Fundamental Design Principles: Redundancy

---

[

]

[CCI per Affidavit 4(a)-(d)]

Adherence to Fundamental Design Principles to Address  
Postulated Failure Mechanisms

# Application of Fundamental Design Principles: Diversity

---

[

]

[CCI per Affidavit 4(a)-(d)]

Adherence to Fundamental Design Principles to Address  
Postulated Failure Mechanisms

[

] [CCI per Affidavit 4(a)-(d)]

Adherence to Fundamental Design Principles to Address  
Postulated Failure Mechanisms

# **B&W mPower Control System Manual Operations**

- [ ] Provided in the mPCS  
[CCI per Affidavit 4(a)-(d)]
  - [ ]
    - ] [CCI per Affidavit 4(a)-(d)]
  - Non-safety Remote Shutdown Panel (RSP) in remote shutdown location inside Reactor Services Building
- Supports Functional Requirements for:
  - Human Factors Goals
  - Safety-related manual control and monitoring of CSFs
  - Remote shutdown capability (GDC 19) due to loss of MCR habitability
- [ ]
  - ] [CCI per Affidavit 4(a)-(d)]

[  
[CCI per Affidavit 4(a)-(d)]

- No credible Single Point Failure disables a safety-related function
- No credible Single Point Failures cause a protective action

- IEEE 603-1991 (incorporated by reference in 10 CFR 50.55a(h):
  - Sections 6.2 and 7.2 require means in the control room to implement manual initiation at the division level of the automatically initiated protective actions. The means provided shall minimize the number of discrete operator manual manipulations
  
- RG 1.62, Revision 1:
  - Means should be provided for the manual initiation of each protective action (e.g., reactor trip, containment isolation) on a division-level basis, regardless of whether means are also provided to initiate the protective action at the component or channel level (e.g., individual control rod, individual isolation valve).
  - An optional acceptable method that satisfies both requirements of IEEE Std 603-1991 and guidance on Point 4 of the NRC position on D3, would be a single safety related manual initiation of protective actions that satisfies Positions 1, 2, 3, 4, 5, 6, and 7 above.
  - By letter dated March 29, 2010 the ACRS issued a recommendation to the NRC Staff: "Revision 1 of RG 1.62 should be revised to state explicitly that a system level actuation of all divisions which meets the requirements of IEEE 603-1991 is acceptable." A clarification was included in revision 1 to RG 1.62:
    - ...However another acceptable method is the system-level manual initiation of protective actions that results in the actuation of all divisions at once. The system-level method is acceptable as long as the requirements for independence, single failure criteria, and minimum equipment in the IEEE Std 603-1991 are met.
  
- BTP 7-19:
  - Point 4: A set of displays and controls located in the main control room should be provided for manual system-level actuation of critical safety functions and for monitoring of parameters that support safety functions. The displays and
  - controls should be independent and diverse from the computer-based safety systems identified in Points 1 and 3.

- Meets Requirements for Safe Shutdown and GDC 19
  - Exists to allow the operator to achieve and maintain safe shutdown in the event that the main control room becomes uninhabitable.  
[ ]
  - Non-safety related [CCI per Affidavit 4(a)-(d)]
  - Means are provided to transfer control to RSP to conform to Fire Hazards Analysis

[

]

[CCI per Affidavit 4(a)-(d)]

# mPower Current Strategy Against Failures

---

[

]

[CCI per Affidavit 4(a)-(d)]

# Trips and Operational Bypasses

[

]

[CCI per Affidavit 4(a)-(d)]

[

]

[CCI per Affidavit 4(a)-(d)]

# Reactor Trip Functions (cont'd)

---

[

]

[CCI per Affidavit 4(a)-(d)]

# Diverse Trips for RTS Functions During Design Basis Events

---

[

# Priority Logic Concepts

[

]

[CCI per Affidavit 4(a)-(d)]

[

[

]

[CCI per Affidavit 4(a)-(d)]

[

]

- Complete Functional Analysis
- Completion of requirements management & analysis
- Understand/synchronize with Chapter 7 DSRS
- Perform Integrated Hazards and Diversity analyses
- Incorporate ESF actuation logic based recent design changes

- **SR** – Source Range, lowest level of reactor power
- **S-R** – safety-related
- **Test Spec** – Test specification, defines the tests required to verify compliance with requirements for a given assembly or system
- **BN** – Business Network
- **PR** – Power Range, highest range of reactor power
- **nS-R** – non-safety-related
- **Req. Spec** – Requirements Specification, normally a module in a requirements database tool, that contains the requirements for the subject assembly or system
- **IR** – Intermediate Range, middle range of neutron flux when measuring reactor power

[

]

[CCI per Affidavit 4(a)-(d)]