U.S. NUCLEAR REGULATORY COMMISSION

DESIGN-SPECIFIC REVIEW STANDARD FOR mPOWER^{TM} iPWR DESIGN

7.0 APPENDIX B INSTRUMENTATION AND CONTROLS - SYSTEM ARCHITECTURE

Introduction

The instrumentation and control (I&C) system architecture provides high-level definition of I&C systems, the assignment of I&C functions to these systems, and the communications between I&C systems. The implementation of the defense-in-depth concept for I&C is achieved mostly at the I&C architectural level. This section provides an approach to describe the I&C system architecture and identifies relevant information to assess the design's conformance to the defense-in-depth concept and the relevant regulations (e.g., Title 10 of the *Code of Federal Regulations*, Section 50.55a(h)). This guidance applies to microprocessor-based technology as well as other forms of complex logic such as programmable logic devices (e.g., Field Programmable Gate Arrays (FPGAs)). This DSRS uses the term software to refer to such technology and complex logic.

Design-Specific Review Standard (DSRS) Chapter 7 sections on the fundamental design principles discuss more specific areas of staff review that take into account the overall I&C architecture. In addition, the actual system development process typically includes, in part, its development life cycle and the development of system architecture descriptions. The application should contain sufficient information on architecture, whether or not a specific platform or technology has been selected, to support the staff's determination of reasonable assurance of safety from the perspective of the fundamental design principles: independence, diversity and defense-in-depth, redundancy, and predictability and repeatability.

Experience has shown that the review of an I&C system design that has a high degree of interconnectivity among computer-based equipment is quite challenging. Without the information related to the overall I&C system architecture, the review of the fundamental design principles may take on a more segmented review approach resulting in a less streamlined, more complicated, and more resource-intensive review effort.

Relevant Information to Support Consideration of I&C Architecture during Design Review

Clause 4 of the Institute of Electrical and Electronics Engineers, Inc. (IEEE) 603 requires, in part, that a specific basis be established for the design of each safety system, including all system functions necessary to fulfill the system's safety intent. The architecture description provides a representation of the I&C system's properties, elements, functions, and the relationship among them. The architectural description should also contain the rationale, justification, or reasoning about architecture decisions that have been made, including potential consequences of such decisions.

The reviewer should consider the I&C system overall architecture in concert with the sections relating to the fundamental design principles. In addition, the reviewer should consider other

ADAMS Accession No. ML12318A201

sections of the DSRS that discuss the I&C system design basis, provide I&C system descriptions, and identify I&C system functions for consistency and additional information.

The reviewer, using engineering judgment that is corroborated in the review of each of the sections of this chapter, should verify that the application contained sufficient information at the architectural level to support a more streamlined review.

The staff should review, as a minimum, the following information, which the application should include:

1. Description of the I&C system architecture. The architecture description should demonstrate that the architecture reflects the fundamental principles of independence, redundancy, D3, and supports deterministic behavior. Regarding safety of the I&C system design, the application should provide sufficient information to demonstrate that the overall architecture proposed sufficiently robust.
2. All I&C functions that are part of the design basis
3. Diagrams of the overall architecture
4. Description of systems necessary to support the defense-in-depth concept of the plant, which provides layers of defensive capabilities to mitigate or prevent potential hazards, including the following:

    A. The I&C systems, including their classification, technologies, boundaries, and interfaces with other systems

    B. End-to-end signal flows and their descriptions (e.g., signal flow paths from sensor input through signal conditioning, data processing, voting, and actuation)

    C. Key functional blocks that make up the I&C architecture, through which the data (plant process information or command signals) are transmitted and their descriptions

    D. Simplified logic diagrams

    E. Signal processing block diagrams and their descriptions

    F. When a vendor's design includes a prioritization scheme that is used to signal selections, the priority functions and their descriptions

    G. Interfaces and comparisons of electrical and I&C diagrams

    H. Specific constraints identified in the I&C design resulting from the general plant safety approach that could affect compliance with regulatory requirements