RIC 2011

Conformance with NRC Regulations and Guidance: Redundancy and Independence for Digital Data Communications

Deanna Zhang
NRC/NRO/DE/ICE1
March 8, 2011

Agenda

- Background
- Regulatory Requirements
- Regulatory Guidance
- Recent Digital Instrumentation and Controls Design Certification and License Reviews
- Design Principles for Data Communications Independence and Redundancy
- Summary

2

Background

- The introduction of digital safety and non-safety systems may enhance plant system functions
- Digital technology allows for increased communication between safety divisions and between safety and non-safety systems.
- Implementation of digital technology may result in challenges to independence and redundancy.
- Interaction between digital systems in different safety divisions and between safety and non-safety systems may result in an increase in the complexity of the safety system architecture.

3

Safety Significance

- Independence and redundancy are fundamental principles used to protect safety critical systems against hazards that may disable the safety function.
  - Such hazards include both anticipated vulnerabilities/ failures and vulnerabilities/failures that might not be anticipated or recognized.
- Without independence and redundancy, hazards from within the safety system or non-safety components can propagate and affect other or all safety components.

4

Regulatory Requirements

- IEEE Std. 603-1991, as incorporated by reference 10 CFR 50.55a(h), requires:
  - Independence between redundant portions of safety systems, and between safety and non-safety systems.
  - Safety systems to meet the single failure criterion.
- 10 CFR Part 50, GDC 24, "*Separation of Protection and Control Systems*"
- 10 CFR Part 50, GDC 21, "*Protection system reliability and testability*"
- "Redundancy" inherently implies "independence"

5

Current NRC Guidance Independence and Redundancy

- The NRC issued Digital Instrumentation and Controls Interim Staff Guidance (D I&C ISG-04) to provide guidance on acceptable implementations of interdivisional communications to meet IEEE Std. 603-1991.
  - Section 1 of D I&C ISG-04: Interdivisional communication
  - Section 3 of D I&C ISG-04: Multidivisional control and display
- RG 1.153 endorses IEEE Std. 379-2000 as an acceptable method for meeting the single-criterion.

6

Recent I&C Design Reviews

- Several proposed new reactor designs use extensive interconnections between safety, control, and monitoring systems.
- Application of these interconnections involve:
  - Sharing information about redundant safety divisions, with the shared information used by the safety function of each division.
  - Multi-divisional display and control of the safety component.
  - Use of non-safety equipment for maintenance and testing of safety systems.
- The use of information originating from, or processed by, the outside division to which it is intended to be redundant may challenge the goal of maintaining independence and redundancy.

7

Regulatory Concerns Regarding Proposed Designs

- A design that meets single-failure criterion does not necessarily meet independence requirements.
- Designs that provide increased reliability (e.g., sharing sensor values) often involve redundant divisions using information from outside the division.
- Several proposed designs create interdivisional dependencies.
- A careful design, combined with a thorough analysis of potential failures, may not sufficiently mitigate the need for meeting certain independence requirements.

8

Design Considerations to Maintain Independence

- Communication between safety divisions and safety and non-safety components should only be implemented to enhance the safety of nuclear power plants.
  - Enhanced system reliability does not equate to increased plant safety
  - Human factors can be utilized to enhance safety
  - Balance between enhanced safety and added complexity
- Demonstrating that the design and development process are of high quality do not ensure that the system is immune to failures and hazards.

9

Design Considerations for Component Redundancy

- Spatial dependencies of variables may inhibit the ability to allow for sufficient redundancy to meet NRC regulations for single failure and equipment maintenance.
- Shared components between safety divisions should be reduced to the lowest set achievable.
- An analysis should be provided that shows how failures of the shared components can be addressed by the safety system.

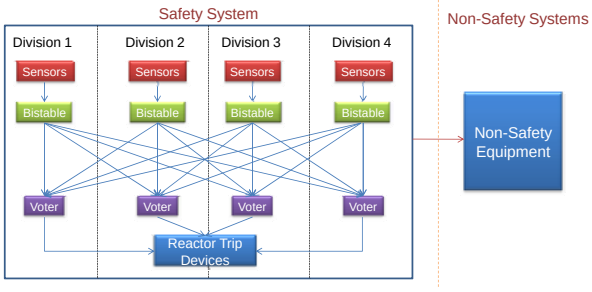
10

Complexity of Design

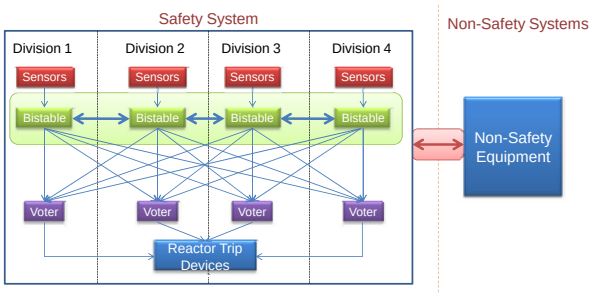
- Ensuring that potential hazards are adequately addressed is difficult in complex systems.
- Many designs have failed due to errors, interactions, and malfunctions that were not anticipated by the designer.
- System complexity does not directly impact independence requirements, though it does increase the level of detail required to demonstrate compliance.
- Applicant should consider the complexity of the design when evaluating if the information provided to demonstrate compliance is adequate.

11

Simple Design to Demonstrate Independence/Redundancy



Complex Design to Demonstrate Independence



Summary

- Modern digital I&C systems offer significant benefits to nuclear power plant operation.
- Digital systems, when implemented without full consideration of potential hazards associated with the system architecture and interdivisional communication, can compromise independence and redundancy, resulting in a loss of safety function.
- Careful design considerations can help mitigate these challenges, allowing for greater use of digital technology.

14

Acronyms

- D I&C: Digital Instrumentation and Controls
- ISG: Interim Staff Guidance
- GDC: General Design Criteria
- CFR: Code of Federal Regulations

15