Digital Instrumentation and Control Interim Staff Guidance Applied to Priority Modules

Terry Jackson, Chief
Instrumentation and Controls Branch 1
Office of New Reactors
RIC 2008 - March 12, 2008

1

WHAT IS A PRIORTY MODULE?

- A device that receives actuation commands from safety and non-safety sources, and sends the command having highest priority to the actuated device.
  - The actuated device is a safety-related component such as a valve, pump, etc
  - Priority logic is implemented with software, firmware, or a combination
  - The priority module must also be safety-related

2

WHY IS A PRIORITY MODULE NEEDED?

- Some reactor vendors are proposing the control of safety equipment from the non-safety control panel/systems for surveillance test, normal operations, etc.
- Also, diverse actuation systems may need to actuate the same safety equipment
- Logic is required to determine which incoming command will have priority to control safety equipment in order to meet NRC requirements

3

DEFENSE-IN-DEPTH/DIVERSITY AND COMMAND PRIORITIZATION

- NRC acceptance of a digital safety system depends on a quality software development process and defense-in-depth/diversity analysis to address the common-cause failure (CCF) potential.
- CCF is a concern since priority modules are located across all divisions and at such a low level in the I&C architecture.
- Digital I&C Interim Staff Guidance (ISG), DI&C-ISG-04, Highly Integrated Control Rooms – Communication Issues, Item 2, "Command Prioritization", specifically provides guidance on use of priority modules among other things.

4

Communications ISG

- Would not have to consider CCF of a hardware-based priority module if the following attributes are addressed:
  - 100 Percent Test Coverage (all combination of binary inputs and internal states)
  - Same tools used to develop the priority module logic are not used for testing
  - Unused inputs should be forced to either "TRUE" or "FALSE"
  - Ensure the completion of a protective action is not interrupted by commands, conditions, or failures outside the priority module's division
  - Safety-related commands that direct a component to a safe state must always have the highest priority and must override all other commands
  - Failure of automatic testing within priority module, whether initiated within or triggered without, should not inhibit safety function
- Software quality assurance documentation is a function of test coverage.

5

NRC Review Experience

- AREVA NP presented a topical report on their priority module called the AV42 Priority Actuation and Control Module.
- NRC staff used DI&C-ISG-04 during the review.
- NRC staff focused on the following technical aspects:
  - Test coverage (inputs, internal states, test boundaries)
  - Test tools, plans, and results
  - Unused pins on logic device
  - Automatic testing
  - Priority logic and other requirements
  - Interfaces and interactions with other components/systems
  - Operating experience

6

Conclusions

- Industry and NRC staff are effectively applying the digital I&C ISG.
- The ISG clarified guidance for system designers and provided a clear roadmap for NRC staff, thus improving review efficiency and effectiveness.
- Experience gained from using the ISG will be used to enhance guidance down the road.

7