ENHANCING SAFETY DURING THE GLOBAL NUCLEAR RENAISSANCE

RIC 2008

DIGITAL I & C
HIGHLY-INTEGRATED CONTROL ROOM COMMUNICATIONS

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

OFFICE OF NUCLEAR REGULATORY RESEARCH

Background

Digital Control and Protection Systems offer extensive opportunities for the sharing and consolidation of information:

- Consolidated workstations via Multidivisional Control and Display units
- Automatic evaluation of measurement deviations among multiple channels
- Data consolidation & archiving
- Communication with maintenance, management, and financial systems

Existing Requirements

Code of Federal Regulations

- 10CFR50.55a(h) invokes IEEE 603 1991: (including the correction sheet dated January 30, 1995)

independence:
- no need for information from other safety or nonsafety divisions to accomplish the safety function
- safety function must be immune to all actions and commands from other safety and nonsafety divisions

… (except for interdivisional voting functions)

isolation:
- no fault or failure in other safety or nonsafety divisions can interfere with safety function

- 10CFR50 Appendix A, GDC 21 "Protection System Reliability and Testability:"

reliability:
- must be designed for high functional reliability commensurate with the safety functions to be performed.

- 10CFR50 Appendix B Criterion III "Design Control:"

quality:
- quality standards must be specified
- design control measures must be provided for verifying or checking the adequacy of design

Regulatory Guide 1.152 (Revision 2, January, 2006) "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants"

- cites IEEE 7-4.3.2 2003 as generally acceptable guidance
- specifically excludes the communication criteria in Annex E

NUREG 0800 (Standard Review plan) (March, 2007)

- Chapter 7 and Appendices address the application of requirements and guidance related to Instrumentation and Controls
  - Appendix 7.1 B: "Guidance for Evaluation of Conformance to IEEE Std 279"
  - Appendix 7.1 C: "Guidance for Evaluation of Conformance to IEEE Std. 603"
  - Appendix 7.1 D: "Guidance for Evaluation of the Application of IEEE Std 7-4.3.2"

Traditional

New Plants

With Digital Interfaces to:

- RPS
- ESFAS
- Safety Control System
- Nonsafety control system
- Monitoring system
- Supervisory system
- Management systems
- Other systems

Considerations in the Transition

Safety System Independence:

- Multiple safety Divisions controlled from a single set of consoles (nonsafety control & display functions)
- Dedicated console for each safety division (for safety control & display functions)
- No cross-divisional interference even with all divisions accessed through a single console
- Communication with outside destinations (including plant LAN/WAN) must not introduce the possibility of interference from outside failures or activities

Communication Process:

- Need to be able to exchange information easily
- Need to ensure that received messages cannot interfere with safety functions
- Need to ensure that communication process cannot interfere with safety functions
- Need to ensure that safety communications (such as exchange of trip status information for multichannel voting) are accurate and timely

Human Factors:

- Navigation – prompt access to needed information and controls
- Presentation – display of information in a meaningful and easily-understood context
- Automation – degree of automation, operator ability to intervene in automated sequences, use of operator-controlled decision/ approval points within automated processes

Nonsafety Functions:

- Safety processors should have minimal nonsafety functions
- Safety division may have separate processors for support functions such as communications

The Digital I&C Project

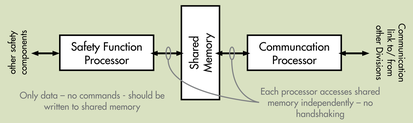
- NRC initiated the Digital I&C Project: 7 Task Working Groups dedicated to specific areas
- Work within and satisfy existing requirements
- TWG 4 addresses communications
  - Goal: take advantage of communications technology within the constraints of existing regulations
  - Many public meetings
  - Extensive discussion of proposed designs
  - TWG 4 issued Interim Staff Guidance on September 28, 2007

Interim Staff Guidance

- Interdivisional Communications
  - Electrical isolation provided via fiber optical connections
  - Separate processors for safety functions & communications
    - > Exchange information via shared memory
    - > No communication of commands or programs (communication cannot alter the execution cycle of the destination processor)
    - > Safety Function processor to be dedicated to safety function, other functions to be minimized
      Example: On-Line Monitoring should be performed by a nonsafety processor, not burden safety processor
  - Engineering / maintenance console should be physically disconnected during normal operation
    - > Nonsafety device with ability to interfere with or alter safety function
- Command Prioritization
  - Selects among multiple commands from multiple independent sources
  - Accommodates safety and nonsafety inputs; safety output, with internal separation and isolation
- Multidivisional Control and Display Stations (not safety related)
  - Interface with safety functions only through priority modules under normal operation
  - Interface with safety processors only when processor is bypassed
  - Supplemented with divisionalized safety-grade control and display stations

Communication Process

- The safety function processor should not be involved in communications, and should be physically incapable of receiving commands or programs by way of the communication link.
- The program execution cycle of the safety function processor should not be impacted by the communication process. In particular, no failure or malfunction of any device or program involved in communications can delay the operation of the safety function processor beyond the timing established in the design bases.



Priority Module

- Prioritization scheme is same as for analog systems.
- Priority Modules include internal isolation and separation as needed for circuits in different safety divisions.
- Signal consolidation function may include minor logic, such as stopping valve motor when fully closed.
- A Priority Module may be used to relay information from safety-related plant equipment to the nonsafety control and monitoring systems.