

United States Nuclear Regulatory Commission Protecting People and the Environment

Digital Instrumentation and Control

December 17, 2015

Speakers

- Victor McCree, Executive Director for Operations, NRC
- John Lubinski, Acting Deputy Office Director for Engineering, NRR
- Richard Stattel, Senior Electronics Engineer, NRR
- John Tappert, Director of Division of Engineering, NRO
- Deanna Zhang, Senior Electronics Engineer, NRO

Agenda

- Background of Digital I&C and Lessons Learned
- Incorporation by Reference of IEEE 603-2009
- Other Key Regulatory Initiatives

Background—Why is Digital Technology Unique?

- Different principles of operation
- Different hazards for digital vs. analog
- Communications independence challenges
- Increased potential for latent errors

Early Actions Taken to Address Digital

- Development of guidance to address unique aspects of digital
 - Regulatory guides on digital I&C system development
 - Standard review plan revision

Formation of the Digital I&C Steering Committee

- Task working groups initiated to address digital I&C licensing process
- Issuance of digital I&C interim staff guidance

What We Learned— Operating Reactors

- Digital I&C licensing processes can be improved
 - Early communications and identification of required documentation works well
 - Graded review approach needs to be improved

What We Learned— New Reactors

- Utilize highly integrated digital I&C systems
- Challenged in providing sufficient design information and analysis to demonstrate safety with initial designs
- Addressing requirements at architectural level was effective

What We Learned— Other Key Issues

- Current I&C requirements should be updated to address digital
- Ambiguities in 10 CFR 50.59 guidance need to be revised
- Diversity and defense-in-depth criteria need to be re-evaluated

The Role of IEEE 603

- Criteria for I&C safety systems
 - Technology neutral
 - Performance based
- Incorporated into regulation
 - Incorporated by reference
 - General Design Criteria

What Changed in the Standard

- New version of the standard adds:
 - Guidance for digital technology
 - Annex on electromagnetic compatibility
 - Guidance for connected equipment
 - Communication independence criteria

Applicability of New Standard

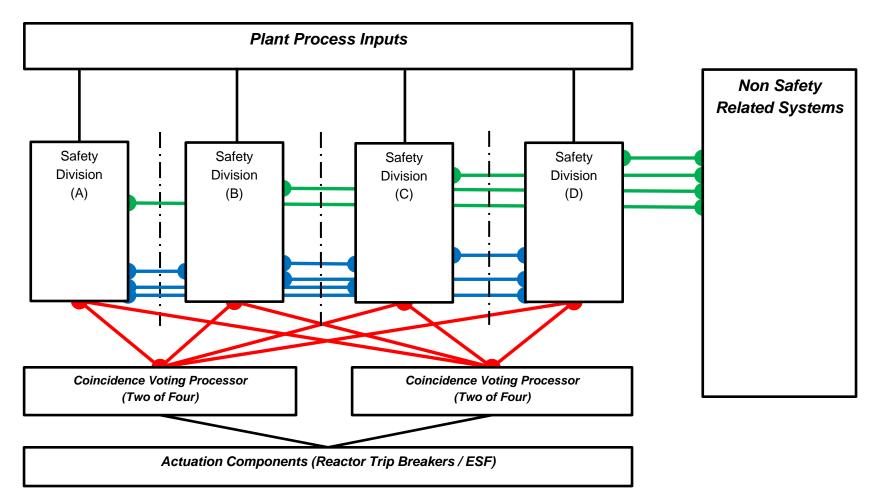
- Conditions for applicability of the new and previously incorporated versions
 - New plant designs required to comply with IEEE 603-2009
 - Impacts operating plants and existing design certifications if changes meet threshold

System Integrity

- Amplify "System Integrity" requirements
- Condition added:

 In order to assure the integrity and reliable operation of safety systems, safety functions shall be designed to operate in a predictable and repeatable manner.

Example Reactor Protection System



Independence

- Amplify "Independence" requirements
 - Between redundant portions of safety systems
 - Between safety systems and other systems

- Amplify "Independence" requirements
 - A. Manner of processing data
 - **B. Detection and mitigation capabilities**

- Amplify "Independence" requirements
 - **C.** For current reactors,

Signals must support safety or provide a safety benefit.

 Amplify "Independence" requirements
D. For new reactors,

(1) One-way—hardware enforced(2) Only signals to perform safety functions are allowed

 Amplify "Independence" requirements

(3) Signals to support diversity and automatic anticipatory reactor trip functions

(4) **Proposed alternatives** requirements

Potential Impact on Operating Plants

- Supports use of newer version of IEEE 603
- Applicants already perform hazard analysis

Potential Impact on New Reactors

- Communication independence demonstrated at higher level
- Limit failure modes and unexpected behaviors associated with communications

Stakeholder Engagement

- NRC staff participated in IEEE 603-2009 development
- ACRS recommended adding conditions
- Industry generally did not support added conditions
- NEI does not support issuance of proposed rule

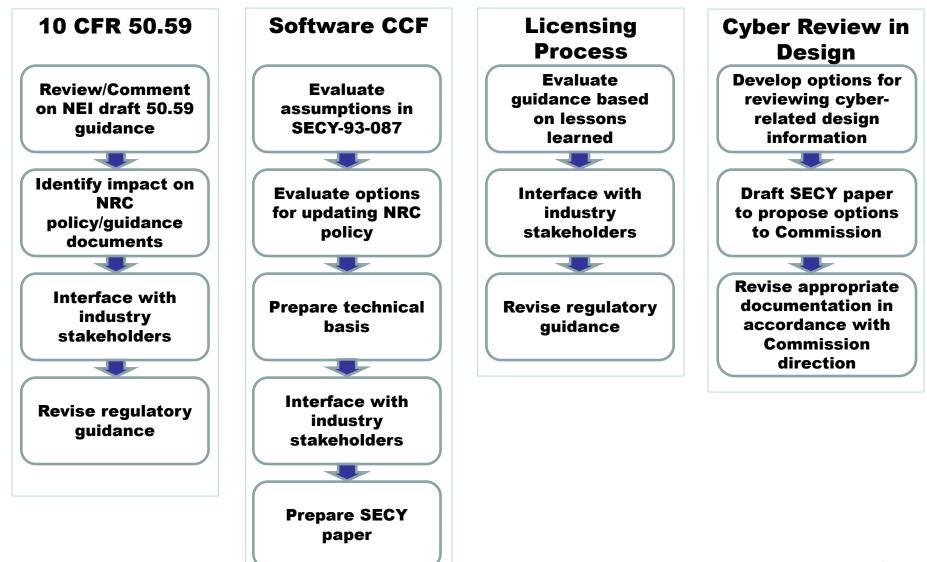
Benefits of Proposed Rule

- Facilitates use of IEEE 603-2009
 - Updates for new technology
 - More effective EMC
- Conditions provide improved consistency and predictability for licensing
- Issuing the proposed rule will facilitate external stakeholder feedback

Key Regulatory Initiatives— Develop a DI&C Action Plan

- Address lessons learned and stakeholder feedback
- Prioritize activities
- Coordinate with industry initiatives

DI&C Action Plan



Enhance 10 CFR 50.59 Guidance

- Non-compliances identified when upgrades performed
- Ensure updated guidance is adequate

How Software Common Cause Failure is Currently Addressed

- SRM-SECY-93-087 defines criteria for addressing software common cause failure
 - BTP 7-19: guidance for implementation
 - NUREG/CR-6303: guidance for performing diversity and defense-indepth analysis

Improve Software Common Cause Failure Criteria

- Evaluate existing policy on software common cause failure
 - Incorporate advances in digital technology
 - Prepare a technical basis paper and a SECY paper
 - Maintain interfaces with industry stakeholders throughout effort

Improve Licensing Process for Digital I&C Systems

- Enhance licensing process in ISG-06 to include lessons from the pilot
- Improve guidance for new reactor licensing processes

Review Cyber Security Design Features During Licensing

- Cyber security design not currently reviewed as part of licensing
- Early consideration of cyber security in the design process is beneficial
- SECY paper under development

Digital I&C Action Plan

- Additional activities:
 - Highly integrated systems
 - Regulatory infrastructure
 - Guidance for alternative evaluation
 - Consistency: licensing and inspections
 - Topical report process

Summary

- Publish proposed rule to obtain stakeholder feedback
- Ensure Digital I&C Action Plan includes key regulatory initiatives
- Coordinate with industry digital I&C working group

Acronyms

- **ACRS Advisory Committee on Reactor Safeguards**
- **BTP Branch Technical Position**
- **CFR Code of Federal Regulations**
- **DI&C Digital Instrumentation and Control**
- **EMC** Electromagnetic Compatibility
- **ESF Engineered Safety Feature**
- **I&C** Instrumentation and Control
- **IEEE** Institute of Electrical and Electronics Engineers
- **ISG Interim Staff Guidance**
- **NEI Nuclear Energy Institute**
- **NRC Nuclear Regulatory Commission**
- **NRO Office of New Reactors**
- **NRR Office of Nuclear Reactor Regulation**
- NUREG NRC technical report
- **SECY** paper Commission Paper
- **SRM Staff Requirements Memorandum**