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

# MP #1 Protection Against Common Cause Failure

Mauricio Gutierrez RES/DE/ICEEB
Dinesh Taneja NRO/DEI/ICE
Rossnyev Alvarado NRR/DE/EICB
Michael Waters, NRR/DE/EICB/Branch Chief

Advisory Committee on Reactor Safeguards
DI&C Subcommittee Briefing
May 17, 2018

# IAP – Modernization Plans

- **Modernization Plan (MP) #1 – Protection Against Common Cause Failure**
  - **MP #1A – Regulatory Issue Summary (RIS) 2002-22, Supplement 1**
  - **MP #1B – Review of NEI 16-16**
  - **MP #1C – Implementing Commission Policy on Protection Against CCF in DI&C Systems**
- MP #2 – Considering Digital Instrumentation & Controls in Accordance with 10 CFR 50.59
- MP #3 – Acceptance of Digital Equipment (Commercial Grade Dedication)
- MP #4 – Assessment for Modernization of the Instrumentation & Controls Regulatory Infrastructure
  - MP #4A – ISG-06 Revision
  - MP #4B – Develop Strategic activities for long-term improvements to the regulatory infrastructure

# Agenda

- **MP #1A** – RIS 2002-22, Supplement 1, "Clarification on Endorsement of Nuclear Energy Institute (NEI) Guidance in Designing Digital Upgrades in Instrumentation and Controls Systems"

- **MP #1B** – Review of NEI 16-16, "Guidance for Addressing Digital Common Cause Failure"

- **MP #1C** – Implementing Commission policy on protection against CCF in DI&C systems

# Background on CCF in DI&C

- DI&C technology can provide advantages in reliability and functionality, but can also create the potential to introduce a software CCF
- Commission directed staff to implement position in SRM to SECY-93-087, II.Q
- Staff implemented Commission direction into staff guidance Branch Technical Position (BTP) 7-19, “Guidance for Evaluation of Diversity and Defense-in-Depth (D3) in Digital-Based Instrumentation and Control System Review Responsibilities”
- SRM to SECY-16-0070

# Technical Issues

- Evolution of digital technology and industry standards
- Evolved scope of applicability
- Addressing CCF concerns when performing upgrades:
  - Determining the amount of emphasis on CCF concerns during system design
  - Determining the likelihood of a CCF
  - Determining the diversity needed
- Determining the need for diverse actuation systems or use of certain design attributes
- Performing a D3 analysis for all types of safety I&C systems under a graded approach
- Addressing CCF concerns in the context of specific 10 CFR 50.59 evaluation criteria

# RIS 2002-22, Supplement 1
# Purpose and Scope

- Clarifies NRC's previous endorsement of NEI 01-01 for 10 CFR 50.59 upgrades
- Clarifies the use of qualitative assessments used to determine that CCF is sufficiently low
- "Sufficiently low" is based on assessing design attributes, quality of the design process and operating experience
- Not applicable to major Reactor Protection System (RPS) and Engineered Safety Features Actuation System (ESFAS) upgrades

# Example RIS Qualitative Factors

- Design Attributes
  - Independence, diversity, etc.
  - Inherent design features such as automated self-testing and watchdog timers
- Quality of the Design Process
  - Use of industry consensus standards shown to be applicable
- Operating Experience
  - Relevant operating experience in similar applications, operating environment or comparable configuration to that of the proposed modification

# RIS 2002-22, Supplement 1 Status & Next Steps

- Initial Draft issued for public comment July 2017.
- Second draft issued for public comment March 2018.
  - Total of 7 commenters
  - Approximately 60 public comments
- Final RIS scheduled for issuance by May 31, 2018.
- Follow-up inspection training and workshops planned.

# NEI 16-16 - Purpose and Scope

- Developed in support of industry response to NRC's activities on Protection Against Common Cause Failure
- NEI 16-16 provides engineering guidance for industry to address CCF concerns. The guidance includes defensive measures that can be credited to address CCF, in addition to those in the current NRC guidance (i.e., BTP 7-19) for both operating and new plants
- Based in part on the design measures in EPRI Technical Report (TR)-3002005326, "Methods for Assuring Safety and Dependability when Applying DI&C Systems"

# NEI 16-16
# Status

- NEI provided second draft to NRC May 2017
- NRC and NEI held joint meetings to discuss and resolve comments.
- In February 2018, NEI requested that NRC pause review of this document.
  - EPRI is revising TR-3002005326.

# Implementing Commission Policy on CCF in DI&C

- Staff will update guidance documents to ensure the Commission policy in SRM to SECY-93-087 continues to be consistently applied and address evolving DI&C technologies
- Staff is not proposing nor requesting a change to Commission policy at this time
- Staff is developing a Commission Information SECY on future improvement efforts in addressing CCF

# Updating Guiding Principles

- Licensees and applicants should continue to address CCFs due to software
- A D3 analysis for RTS and ESFAS to address CCF concerns continues to be required. This analysis can be either a best estimate (i.e., using realistic assumptions) or a design basis analysis
- Clarify the use of a graded approach for a D3 analysis for less safety critical systems
- Clarify the use of alternate means to address CCF concerns
- Clarify the use of certain design attributes to address CCF concerns

# Next Steps

- Hold stakeholder interactions
- Apply staff clarifications in all activities for regulatory guidance and endorsement activities
  - Issue RIS 2002-22 supplement for 50.59
  - Review of NEI 96-07 Appendix D for 50.59
  - Standard Review Plan (SRP) and/or BTP 7-19 update
  - Review of future industry guidance (e.g., NEI 16-16)
- Provide Info SECY to Commission (August 2018)

# Broader Modernization Activities

- Advanced Reactor Framework
- Research is being performed to evaluate I&C aspects that offers opportunities for potential enhancements in the NRC regulatory infrastructure:
  - Risk informed approach
  - Embedded Digital Devices and Evolving Technologies
  - Technical Basis for Addressing CCF

# Questions?

# End

# Acronyms

- ACRS – Advisory Commission on Reactor Safeguards
- ADAMS - Agencywide Document Access and Management System
- ALS – Advanced Logic System
- AOO – Anticipated Operational Occurrence
- BTP – Branch Technical Position
- CCF – Common Cause Failure
- CFR – Code of Federal Regulations
- DCPP – Diablo Canyon Power Plant
- DI&C – Digital Instrumentation and Control
- D3 – Diversity and Defense-in-Depth
- DSRS – Design Specific Review Standard
- EDD – Embedded Digital Devices
- EPRI _ electric Power Research Institute
- ESFAS – Engineering Safety Features Actuation System
- IAP – Integrated Action Plan
- I&C – Instrumentation and Control
- IEEE – Institute of Electrical and Electronics Engineers
- ISG – Interim Staff Guidance
- MP – Modernization Plan
- NEI – Nuclear Energy Institute
- NRC – Nuclear Regulatory Commission
- PPS – Process Protection System
- RPS – Reactor Protection System
- RIS – Regulatory Issue Summary
- RTS – Reactor Trip System
- SRM – Staff Requirements Memorandum
- SSC – Structures, systems, and components
- TR – Technical Report