

Path Forward on Protection Against Common Cause Failure

Mauricio Gutierrez, RES/DE/ICEEB

Dinesh Taneja, NRO/DEI/ICE

Rossnyev Alvarado, NRR/DE/EICB

NRC Public Meeting

May 24, 2018

IAP – Modernization Plan #1

- Goal – Evaluate the NRC’s existing positions on acceptable defenses against common cause failure (CCF) within digital instrumentation and controls (DI&C) systems and measures that can be applied to prevent or mitigate against a potential CCF within DI&C safety and non-safety systems.
 - **MP #1A** – Supplement to Regulatory Issue Summary (RIS) 2002-22 to clarify endorsement of NEI 01-01
 - **MP #1B** – Review of Nuclear Energy Institute (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 Staff Requirements Memorandum (SRM) to SECY-93-087, II.Q
- Staff implemented Commission direction into BTP 7-19, “Guidance for Evaluation of Diversity and Defense-in-Depth in Digital-Based Instrumentation and Control System Review Responsibilities”
- SRM to SECY-16-0070

Stakeholder Interactions and Feedback on CCF

- Integrated Action Plan (IAP) development and revision interactions.
- Industry submitted white paper on CCF in DI&C.
- Industry Comments and Proposed Revisions to BTP 7-19
- Interactions on NEI 16-16 Drafts 1 and 2
- Interactions on Supplement RIS 2002-22
- Consideration of international practices

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 Diversity and Defense in Depth (D3) analysis for all types of safety I&C systems under a graded approach
- Addressing CCF concerns in the context of specific 10 Code of Federal Regulations (CFR) 50.59 evaluation criteria

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 requesting a change to Commission policy at this time
- Staff is developing an Information paper on future improvement efforts in addressing CCF

Updating Guiding Principles

- Licensees and applicants should continue to address CCFs
- 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

- Provide information paper to the Commission (August 2018)
- Update Integrated Action Plan (September 2018)
- Apply guiding principles in all regulatory guidance development and endorsement activities.
 - Update BTP 7-19 (start Fall 2018)
 - Review of future industry guidance (e.g., NEI 16-16)
- Hold table top workshops and training activities for NRC staff and industry.
- Broader Modernization and Research activities

Path forward – Schedule MP #1C

Ensuring Commission policy on defense against CCF in digital I&C systems is consistently applied.

	Activity	Schedule
C.1	Begin staff review to identify specific aspects of NRC’s position on CCF and communicate any policy issues that need to be modified. Meet with DI&C Steering Committee and other stakeholders as needed.	April-July 2017 (c)
C.2	Develop and finalize list of specific aspects of NRC’s position on CCF impacted by review of NEI 16-16 draft updates and alert Commission of policy issues that will require attention.	April - August 2017(c)
C.3	Begin development of SECY on recommendations regarding NRC policy to protect digital I&C systems against CCF concerns.	September 2017 (c)
C.4	Present Status Update to ACRS DI&C Subcommittee	May 17, 2018 (c)
C.5	Status Update Public Meeting	May 24, 2018
C.6	Begin Finalization of INFO SECY	July 18, 2018
C.7	Submit information paper to the Commission	Mid August 2018

Questions?

Acronyms

BTP – Branch technical position

CCF – Common cause failure

CFR – Code of federal regulations

D3 – Diversity and defense-in-depth

DI&C – Digital instrumentation and control

EPRI – Electric Power Research Institute

ESFAS – Engineered safeguard actuation system

IAP – Integrated action plan

MP – Modernization plan

NEI – Nuclear Energy Industry

RTS – Reactor trip system

SRM – Staff record memorandum

SRP – Standard review plan

TR – Technical report

End