Common Cause Failure Policy

Alan Campbell
Technical Advisor

NUCLEAR ENERGY INSTITUTE

State of Digital I&C

- The Digital I&C Integrated Action Plan (IAP) has improved regulatory guidance clarity and consistency
  - RIS 2002-22 Supplement 1 provided criteria for qualitative assessments of Common Cause Failure (CCF) in low safety significant safety-related systems.
  - BTP 7-19 Revision 8 incorporated graded approach assessments into staff review guidance
  - NEI 96-07, Appendix D and Reg. Guide 1.187 Rev. 3 provided enhanced guidance for digital systems under 50.59
  - DI&C-ISG-06 Rev. 2 provided an Alternate Review Process to improve regulatory confidence for digital safety systems upgrades.

Treatment of Digital I&C

- Addressing CCF in complex High Safety Significant Safety-Related I&C Systems remains a barrier that must be overcome
- SRM/SECY-93-087 provides digital CCF policy.
- BTP 7-19 provides review guidance describing acceptable methodologies to meet digital CCF policy.
- BTP 7-19 Rev. 8 prescribes one of the following:
  - Diversity
  - Testing – BTP-7-19 Acceptance Criteria are not possible for complex systems, for example *“every possible executable logic path (includes nonsequential logic paths)”*

Prescribed Diversity

- Prescribed diversity does not address initial NRC concerns documented in SECY-91-292, *Digital Computer Systems for Advanced Light Water Reactors*
  - Lack of experience in nuclear applications
  - Absence of requirements and standards related to digital-specific design aspects
  - Lack of guidance and standards related to software development processes
- These concerns are not applicable today.

Prescribed Diversity (cont.)

- Other issues with current approach:
  - Lack of clear acceptance criteria:
    - NUREG/CR-6303 describes 6 attributes to diversity to be considered, but does not provide acceptance criteria
  - Application of diversity does not improve digital control system reliability
  - Adds cost barrier to upgrading critical safety systems

Why Digital Safety Systems?

- Existing systems are reaching obsolescence (or have already passed it)
- Enhances safety via system diagnostic capabilities to identify and respond to issues
- Improves plant performance via improved accuracy, processing time, and automated capabilities
- Provides more data available to Operations, Maintenance and Engineering resulting in better real-time knowledge
- Reduces hardware inventory compared to existing systems

Supports long-term, safe operation of our plants

Today's Digital Landscape

- Digital I&C technology has design features that provide for deterministic behaviors through the use modern standards
- International standards, such as IEC/IEEE, are widely accepted and have stable processes to reflect current understanding
- Hazard analysis techniques have matured and are used extensively in non-nuclear safety industries (such as aviation/aerospace, defense, automotive, and chemical industries)

NRC needs a modernized digital CCF policy that reflects today's technology, experience, and understanding

SRM/SECY-93-087

Policy Summary

- SRM/SECY-93-087 Four Position Policy
  1. Assess defense-in-depth and diversity to demonstrate CCF vulnerabilities are addressed
  2. Analyze each CCF vulnerability for each accident analysis event and demonstrate diversity
  3. Provide a diverse means for each CCF vulnerability that could disable a safety function. Diverse means can be non-safety related
  4. Provide diverse and independent MCR displays and controls for manual, system level actuation of critical safety function

SRM/SECY-93-087 Position 1

1. The applicant shall assess the defense-in-depth and diversity of the proposed instrumentation and control system to demonstrate that vulnerabilities to common-mode failures have adequately been addressed

SRM/SECY-93-087 Position 1

- Remains applicable and provides high-level requirement to evaluate “common-mode failures”
- Industry Proposal
  - Remove “diversity”
    - “Defense-in-depth” adequately encompasses the assessment
  - Limit scope of policy to complex High Safety Significant Safety-Related systems
  - Specify the policy is intended to address “digital common cause failures”
  - Update “common-mode failures” to “common cause failures”

Proposed Position1

1. The applicant shall assess the defense-in-depth ~~and diversity~~ of the proposed complex high safety significant safety-related instrumentation and control system to demonstrate that vulnerabilities to digital common ~~mode~~ cause failures have adequately been addressed

RPS/ESFAS Upgrade Example:
There is no change to the application of this policy to a complex high safety significant safety-related upgrade from these changes. Existing guidance for low safety significant safety-related systems in RIS 2002-22 Supplement 1 and BTP 7-19 is sufficient for applicable systems.

SRM/SECY-93-087 Position 2-4

2. In performing the assessment, the vendor or applicant shall analyze each postulated common-mode failure for each event that is evaluated in the accident analysis section of the safety analysis report (SAR) using best-estimate methods. The vendor or applicant shall demonstrate adequate diversity within the design for each of these events
3. If a postulated common-mode failure could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common-mode failure, shall be required to perform either the same function or a different function. The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions
4. A set of displays and controls located in the main control room shall be provided for manual, system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. The displays and controls shall be independent and diverse from the safety computer system identified in items 1 and 3 above

SRM/SECY-93-087 Position 2-4 Summary

2. Analyze each CCF vulnerability for each accident analysis event and demonstrate diversity
3. Provide a diverse means for each CCF vulnerability that could disable a safety function. Diverse means can be non-safety related
4. Provide diverse and independent MCR displays and controls for manual, system level actuation of critical safety function

SRM/SECY-93-087 Position 2-4

- Industry Proposal:
  - Provide for two acceptable pathways
  - Pathway 1:
    - Maintain current SRM/SECY-93-087 approach
    - Consolidate positions 2-4 into point 2.a
    - Replace “safety computer system” with “digital safety system”
    - Update “common-mode failure” to “common cause failure”
  - Pathway 2:
    - Add risk-informed, performance-based approach as point 2.b

Proposed Position 2.a

2. In performing the assessment, the vendor or applicant shall perform one of the following:

    a. Analyze each postulated common ~~-mode~~ cause failure for each event that is evaluated in the accident analysis section of the safety analysis report (SAR) using best-estimate methods. The vendor or applicant shall demonstrate adequate diversity within the design for each of these events

    If a postulated common ~~-mode~~ cause failure could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common ~~-mode~~ cause failure, shall be required to perform either the same function or a different function. The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions

    A set of displays and controls located in the main control room shall be provided for manual ~~, system-level~~ actuation of critical safety functions and monitoring of parameters that support the safety functions. The displays and controls shall be independent and diverse from the digital safety ~~computer~~ system ~~identified in items 1 and 3 above~~

Proposed Position 2.a Example

- RPS/ESFAS Upgrade Example:
  - There is no change to the application of this policy to a complex high safety significant safety-related upgrade from these changes.
  - The applicant will continue to:
    - perform a NUREG/CR-6303 analysis
    - implement a diverse means for CCF that can disable safety functions
    - implement diverse and independent displays and controls in the Main Control Room (MCR) for manual actuation

Proposed Position 2.b

2. In performing the assessment, the vendor or applicant shall perform one of the following:

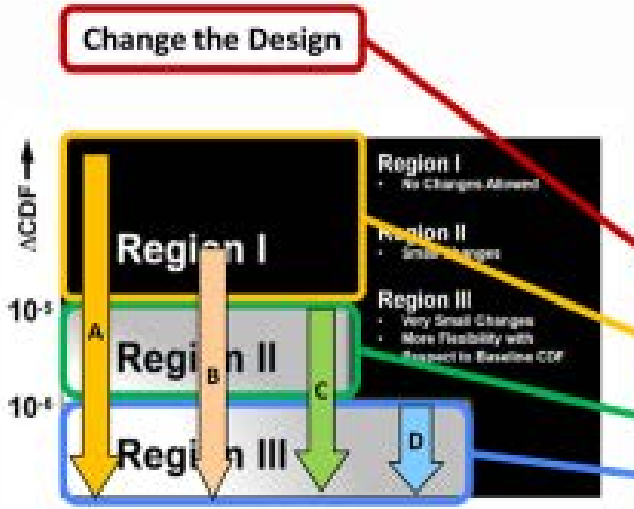
    b. Identify each common cause failure that could disable a safety function using risk-informed hazards analysis techniques. Commensurate with the risk significance of each identified CCF, the applicant shall demonstrate adequate measures, such as design attributes, diversity or testing, to address the potential cause of the CCF that could disable a safety function or the resulting event.

    The measures may be performed by non-safety systems or components if they are of sufficient quality and can reliably perform the necessary functions and with a documented basis that the measures are unlikely to be subject to the same common cause failure.

Proposed Position 2.b Example

- RPS/ESFAS Upgrade Example Using NEI 20-07 Rev. D:
- The applicant will:
  - perform a PRA sensitivity study to determine the impact of each system failure on Core Damage Frequency and Large Early Release Frequency.
  - map results to RG 1.174 regions (as described in RG 1.174 Figures 4 and 5)
  - apply systems theoretic process analysis techniques to model the system and determine specific scenarios leading to failures.
  - apply measures to address each scenario commensurate with results of PRA sensitivity study and mapping.

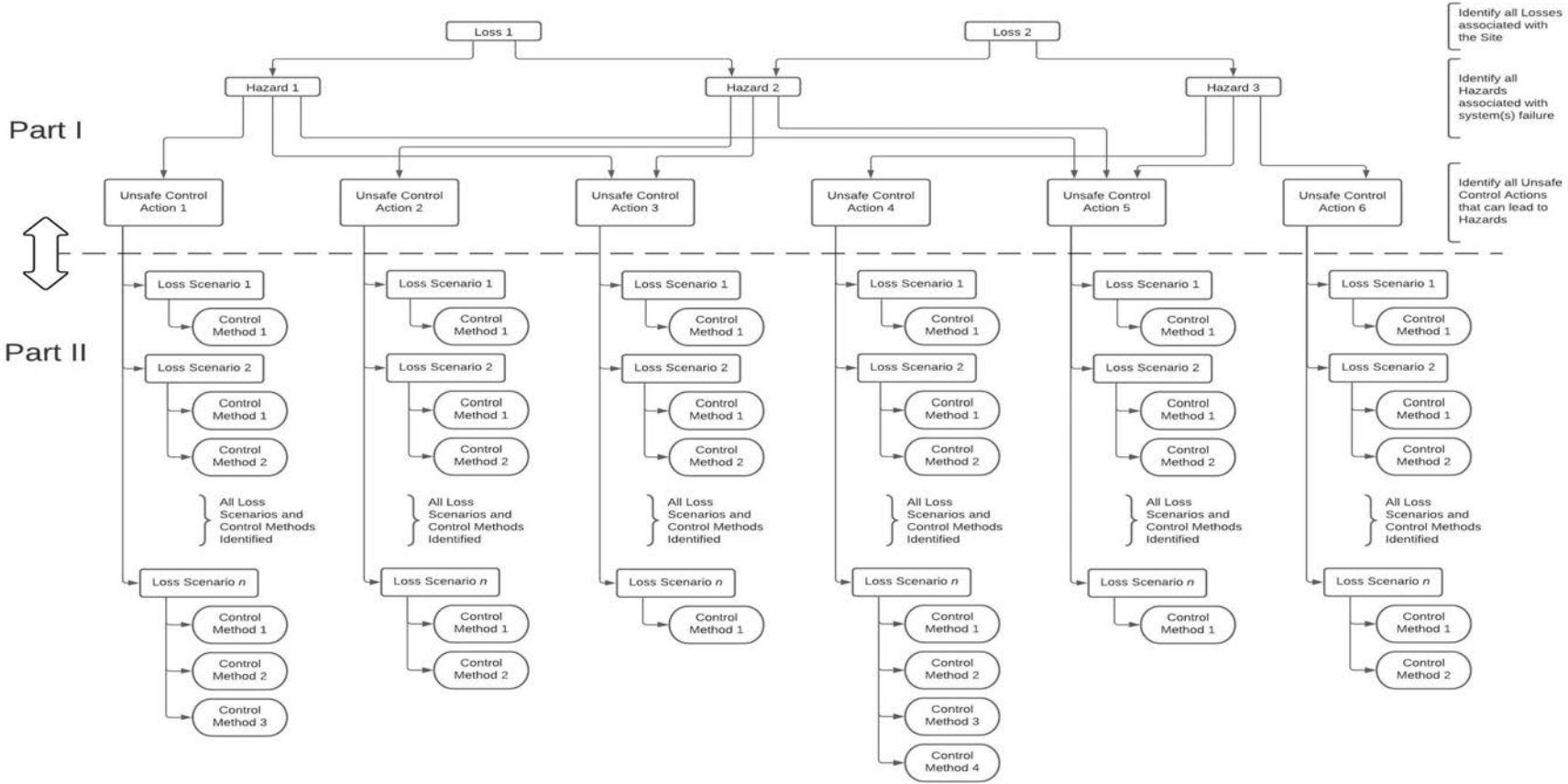
Proposed Position 2.b Example



Risk Reduction Objectives

RRO	Change in Core Damage Frequency – CDF (per year)	Change in Large Early Release Frequency – LERF (per year)
Change the Design	ΔCDF > 1E-3	ΔLERF > 1E-4
A	1E-4 < ΔCDF ≤ 1E-3	1E-5 < ΔLERF ≤ 1E-4
B	1E-5 < ΔCDF ≤ 1E-4	1E-6 < ΔLERF ≤ 1E-5
C	1E-6 < ΔCDF ≤ 1E-5	1E-7 < ΔLERF ≤ 1E-6
D	ΔCDF ≤ 1E-6	ΔLERF ≤ 1E-7

Proposed Position 2.b Example



NEI Path Forward

Consider public meeting dialogue

Update proposed CCF policy, as needed

Issue NEI recommendation to NRC via transmittal letter