NEI TECHNICAL REPORT

NEI 20-07, Rev E

Guidance for Addressing Common Cause Failure in High Safety-Significant Safety-Related Digital I&C Systems

Prepared by the Nuclear Energy Institute
July 2023

Revision Table

Revision	Description of Changes	Date Modified	Responsible Person
Rev E	Updated to account for SRM-SECY-22-0076. Restructured to support safety case development.	7/21/23	Campbell, Alan

Acknowledgements

This document was developed by the Nuclear Energy Institute. NEI acknowledges and appreciates the contributions of NEI members and other organizations in providing input, reviewing, and commenting on the document including:

NEI Project Lead:	Alan Campbell, NEI
NEI Project Team:	Warren Odess-Gillett, Westinghouse
	Neil Archambo, Archambo EC
	Ray Herb, Southern Nuclear Company
	Jeremy Chenkovich, Dominion Energy
	Mark Samselski, Constellation Energy

Notice

Neither NEI, nor any of its employees, members, supporting organizations, contractors, or consultants make any warranty, expressed or implied, or assume any legal responsibility for the accuracy or completeness of, or assume any liability for damages resulting from any use of, any information apparatus, methods, or process disclosed in this report or that such may not infringe privately owned rights.

Executive Summary

Common Cause Failure (CCF) in High Safety-Significant, Safety-Related (HSSSR) Digital Instrumentation and Control (DI&C) Systems is a significant technical and regulatory issue that must be overcome to modernize the existing operating nuclear power plants and enable new reactor technology to be deployed. Historically, CCF has been addressed through the implementation of independent and diverse Instrumentation and Control (I&C) systems. The use of independent and diverse I&C systems may address some sources of CCF, but these systems do not sufficiently address other sources of CCF. Additionally, diverse I&C systems add complexity to the facility, divert resources from safety-significant activities, and increase Operations and Maintenance (O&M) costs. Independence and diversity are indeed useful design techniques; however, these design techniques should be used when supported by an engineering analysis. The Commission provided direction to NRC staff in SRM-SECY-22-0076 documenting an expanded policy that allows for new approaches to addressing CCF using risk insights. NEI 20-04, "The Nexus Between Safety and Operational Performance in the U.S. Nuclear Industry," provides data that displays the impact of risk-informed initiatives on the U.S. nuclear industry. Between 1992 and 2020, the U.S. nuclear industry reduced Core Damage Frequency (CDF) on average by a factor of 10. Focusing on safety significant issues allows the allocation of resources in the manner that most effectively improves safety.

This document provides a process for developing a new type of Diversity and Defense-in-Depth (D3) analysis. This document establishes a safety case using claims, arguments, and evidence to demonstrate that vulnerabilities to digital CCF have been adequately addressed. The safety case depends on outputs from EPRI engineering and diagnostic tools to provide evidence that supports claims and arguments described in this document. To prove that vulnerabilities to CCF have been adequately addressed, the D3 analysis must be able to demonstrate that:

1. Credible and likely sources of potential CCF have been identified and analyzed.
2. Each source of potential CCF has been reasonably prevented, mitigated, or adequately dispositioned.

This document provides the safety case which provides the details that demonstrate the output of the EPRI Digital Engineering Guideline (DEG), Hazards and Consequence Analysis in Digital Systems (HAZCADS), and Digital Reliability Analysis Methodology (DRAM) processes (References 13, 14, and 15) provide a D3 analysis addressing the SRM-SECY-22-0076 policy. The safety case described within this document is broken into 3 "tiers" for descriptive purposes.

- Tier 1 establishes the primary objective of demonstrating that potential vulnerabilities of CCF have been adequately identified.
- Tier 2 provides sub-claims and arguments that demonstrate the efficacy of the EPRI HAZCADS and DRAM processes to identify and establish the criteria for each applicant to demonstrate they adequately executed these processes.
- Tier 3 will be completed by each applicant using this methodology. Tier 3 will consist of the arguments, and associated evidence required to complete the safety case using application-specific results from the EPRI HAZCADS and DRAM processes.

The completed safety case (i.e., this document AND the application specific Tier 3 information) constitutes a D3 analysis demonstrating that CCF in a HSSSR DI&C system has been adequately identified and addressed.

Table of Contents

Table of Figures

[redacted]

Table of Tables

[redacted]

1 INTRODUCTION

Common Cause Failure (CCF) in High Safety-Significant, Safety-Related (HSSSR) Digital Instrumentation and Control (DI&C) Systems is a significant technical and regulatory issue that must be overcome to modernize the existing operating nuclear power plants and enable new reactor technology to be deployed. Historically, CCF has been addressed through the implementation of independent and diverse Instrumentation and Control (I&C) systems. The use of independent and diverse I&C systems may address some sources of CCF, but these systems do not sufficiently address other sources of CCF. Additionally, diverse I&C systems add complexity to the facility as well as increase Operations and Maintenance (O&M) costs. Independence and diversity are indeed useful design techniques; however, these design techniques should be used when supported by an engineering analysis. The Commission provided direction to NRC staff in SRM-SECY-22-0076 documenting an expanded policy that allows for new approaches to addressing CCF using risk insights. NEI 20-04, "The Nexus Between Safety and Operational Performance in the U.S. Nuclear Industry," provides data that displays the impact of risk-informed initiatives on the U.S. nuclear industry. Between 1992 and 2020, the U.S. nuclear industry reduced Core Damage Frequency (CDF) on average by a factor of 10. Focusing on safety significant issues allows the allocation of resources in the manner that most effectively improves safety.

This document provides a process for developing a new type of Diversity and Defense-in-Depth (D3) analysis. This document establishes a safety case using claims, arguments, and evidence to demonstrate that vulnerabilities to digital CCF have been adequately addressed. This document provides the safety case which provides the details that demonstrate the output of the EPRI Digital Engineering Guideline (DEG), Hazards and Consequence Analysis in Digital Systems (HAZCADS), and Digital Reliability Analysis Methodology (DRAM) processes (References 13, 14, and 15) provide a D3 analysis addressing the SRM-SECY-22-0076 policy.

This process may be applied to operating reactor licensees or new plant applicants. Licensees and applicants should ensure the DI&C system design meets all other applicable regulatory requirements and applicable guidance. Applicants using this guidance for operating reactor license amendments and new plant applications using NUREG-0800 Standard Review Plan guidance can use this guidance to develop a D3 assessment to demonstrate that CCF has been adequately addressed. Applicants using this guidance for new plant applications using Regulatory Guide 1.233 can use this guidance to develop a D3 assessment to demonstrate the adequacy of special treatments applied to address CCF.

2 DEFINITIONS

Core Damage Frequency (CDF) – An expression of the likelihood that, given the way a reactor is designed and operated, an accident could cause the fuel in the reactor to be damaged.

Digital Common Cause Failure (CCF) – A latent design defect in active hardware components, software, or software-based logic resulting in a loss of function to multiple structures, systems, or components.

High Safety Significant Safety-Related (HSSSR) – Safety-related systems, structures, or components (SSCs) that perform safety-significant functions (e.g., Reactor Protection Systems and Engineered Safety Features Actuation Systems). These SSCs have one or more of the following: 1. Credited in FSAR to perform design functions that significantly contribute to plant safety; 2. Relied upon to initiate and complete control actions essential to maintaining plant parameters within acceptable limits for a Design Basis Event or maintain the plant in safe state after safe shutdown; and 3. Failure could directly lead to accident conditions that have unacceptable consequences. Systems categorized as Risk Informed Safety Category 1 (RISC-1) in accordance with Regulatory Guide 1.201 are HSSSR.

Large Early Release Frequency (LERF) – An expression of the likelihood that an event involving a rapid, unmitigated release of airborne fission products from the containment to the environment that occurs before effective implementation of offsite emergency response, and protective actions, such that there is a potential for early health effects.

Software – The programs used to direct operations of a programmable digital device. Examples include computer programs and logic for programmable hardware devices, and data pertaining to its operation.

System Theoretic Process Analysis (STPA) – a hazard analysis technique developed by MIT that is based on systems engineering principles. It is a hazard analysis method that is part of a set of safety engineering methods developed by MIT under the umbrella heading of Systems-Theoretic Accident Model and Processes (STAMP).

The following definitions are from EPRI HAZCADS, EPRI DRAM and the STPA Handbook:

Control Method: The ad hoc, policy-based, plant procedure based, or technical features, functions, and capabilities that can be implemented to mitigate risk by protecting a system from a random or systematic failure, or detecting, responding, and recovering from a random or systematic failure.

Control Structure: A hierarchical control structure is a system model that is composed of feedback control loops. An effective control structure will enforce constraints on the behavior of the overall system.

Hazard: A system state or set of conditions that, together with a particular set of worst-case environment conditions, will lead to an accident (loss). This definition is broader than the scope of what constitutes a "hazard" in the PRA.

Loss: A loss involves something of value to stakeholders. Losses may include a loss of human life or human injury, property damage, environmental pollution, loss of mission, loss of reputation, loss or leak of sensitive information, or any other loss that is unacceptable to the stakeholders.

Loss Scenario – A loss scenario describes the causal factors that can lead to unsafe control actions and to hazards.

Random Loss Scenario – A loss scenario caused by a random hardware failure. When a random loss scenario is not mitigated, the related unsafe control action (UCA) is a Single Point Vulnerability.

Risk Reduction Target (RRT) – Risk reduction to be achieved by the […] safety-related systems and/or other risk reduction measures in order to ensure that the tolerable risk is not exceeded.

Systematic Failure – Failure, related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation, or other relevant factors.

Systematic Loss Scenario – A loss scenario caused by a failure that happens in a deterministic (non-random) and predictable fashion from a certain cause, which can only be eliminated by a modification of the design, operating procedures, or other relevant factors. When a systematic loss scenario is not mitigated, and the related unsafe control action (UCA) can occur in multiple redundancies of I&C equipment, the result is a common cause failure (CCF). Systematic loss scenarios are mitigated by the allocation of systematic control methods.

Unsafe Control Action (UCA): A control action that, in a particular context and worst-case environment, will lead to a hazard.

3 REGULATORY BASIS

[redacted]

[redacted]

[redacted]

- [redacted]

  [redacted]

- [redacted]

  [redacted]

  [redacted]

- [redacted]

[redacted]

[redacted]

[redacted]

[redacted] [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

4 SYSTEM DIAGNOSTIC PROCESS

[redacted]

[redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]

[redacted]

[redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted] [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted] [redacted]

[redacted] [redacted]

[redacted] [redacted]

[redacted] [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

- [redacted]
  - [redacted]
  - [redacted]
- [redacted]
  - [redacted]
  - [redacted]

[redacted]

[redacted]

[redacted] [redacted]

[redacted]

[redacted] [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]

5 SAFETY CASE DEVELOPMENT

[redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

- [redacted]

  [redacted]

- [redacted]

  [redacted]

- [redacted]

  [redacted]

[redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]

[redacted]

[redacted]

[redacted] [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted] [redacted]

[redacted]

[redacted]

[redacted] [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted] [redacted]

[redacted]

[redacted] [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

- [redacted]
- [redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

[redacted]

[redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted] [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted] [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

> [redacted]

[redacted]

[redacted] [redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]

[redacted]

[redacted] [redacted]

[redacted]

> [redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]

[redacted]

[redacted] [redacted]

[redacted]

> [redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]

[redacted]

[redacted]

[redacted] [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted] [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

6 CONCLUSION

Using DI&C system design documentation provided from EPRI DEG output documents, the EPRI HAZCADS process is effective at identifying Stakeholder Losses, System Hazards, UCAs and RRTs. UCAs that are present in multiple redundancies of a DI&C system and impact core damage or large early releases are considered CCF. This process is effective at identifying the most likely and credible CCFs at a nuclear power plant. EPRI DRAM uses the EPRI HAZCADS results to identify Systematic Loss Scenarios that may lead to each CCF. Using the RRT and Systematic Loss Scenarios, Control Methods are applied to each causal factor commensurate with the risk significance identified.

The safety case provided within this document presents a clear, logical approach to demonstrating that vulnerabilities to CCF have been adequately addressed in DI&C systems for both operating and new reactors. The safety case provides the claims, arguments, and evidence necessary to demonstrate alignment with the Commission direction in SRM-SECY-22-0076.

7 REFERENCES

1. 10 CFR Part 50, “Domestic Licensing of Production and Utilization Facilities”
2. 10 CFR Part 50, Appendix A, “General Design Criteria for Nuclear Power Plants”
3. 10 CFR Part 50, Appendix B, “Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants”
4. 10 CFR Part 50.12, “Specific exemptions”
5. 10 CFR Part 50.54, “Conditions of licenses”
6. 10 CFR Part 50.55a, “Codes and standards”
7. 10 CFR Part 50.59, “Changes, tests and experiments”
8. 10 CFR Part 52, “Licenses, certifications, and approvals for nuclear power plants”
9. DI&C-ISG-06, “Digital Instrumentation and Controls Interim Staff Guidance, Revision 2, December 2018, U.S. NRC ADAMS Accession # ML18269A259
10. EPRI Report 3002000509, “Hazard Analysis Methods for Digital Instrumentation and Control Systems,” Revision 0, June 2013
11. EPRI Report 3002004995, “Program on Technology Innovation: Analysis of Hazard Models for Cyber Security: Phase I,” Revision 0, Nov. 2015
12. EPRI Report 3002004997, “Program on Technology Innovation: Cyber Hazards Analysis Risk Methodology, Phase II: A Risk Informed Approach,” Revision 0, Dec. 2015

13. EPRI Report 3002011816, “Digital Engineering Guide – Decision Making Using Systems Engineering,” Revision 0, January 2021

14. EPRI Report 3002016698, “HAZCADS: Hazards and Consequences Analysis for Digital Systems,” Revision 1, July 2021

15. EPRI Report 3002018387, “DRAM: Digital Reliability Analysis Methodology,” Revision 0, July 2021

16. IAEA NP-T-3.27, “Dependability Assessment of Software for Safety Instrumentation and Control Systems at Nuclear Power Plants,” 2018

17. IEC 61508, Edition 2.0, 2010-04, “Functional Safety of Electrical/Electronic/Programmable Electronic Safety Related Systems”

18. IEEE 279-1971, “Criteria for Protection Systems for Nuclear Power Generating Stations”

19. IEEE 603-1991, “Criteria for Safety Systems for Nuclear Power Generating Stations”

20. ISO/IEC/IEEE 15026-2:2022, “Systems and software engineering – Systems and software assurance – Part 2: Assurance case”

21. MIT Partnership for Systems Approaches to Safety and Security (PSASS), 2023 STAMP Workshop General Information (http://psas.scripts.mit.edu/home/2023-stamp-workshop-information/)

22. NEI 20-04, “The Nexus Between Safety and Operational Performance in the U.S. Nuclear Industry,” March 2020

23. NUREG-0800, Branch Technical Position (BTP) 7-19, “Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems,” Revision 8, Jan. 2021

24. NuScale Standard Plant Final Safety Analysis Report, Chapter Seven, Instrumentation and Controls, Part 2 – Tier 2, NuScale Power, ADAMS Accession # ML20224A495

25. NuScale Final Safety Evaluation Report, Chapter Seven, Instrumentation and Controls, ADAMS Accession # ML20204B028

26. Regulatory Guide 1.174, “An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis,” Revision. 2, May 2011

27. Regulatory Guide 1.200, “Acceptability of Probabilistic Risk Assessment Results for Risk-Informed Activities,” Revision 3, Dec. 2020

28. Regulatory Guide 1.201, “Guidelines for Categorizing Structures, Systems, and Components in Nuclear Power Plants According to Their Safety Significance,” Revision 1, May 2006

29. Regulatory Guide 1.233, “Guidance for a Technology-Inclusive, Risk-Informed, and Performance-Based Methodology to Inform the Licensing Basis and Content of Applications for Licenses, Certifications, and Approvals for Non-Light Water Reactors,” Revision 0, June 2020

30. SafetyHAT: A Transportation System Safety Hazard Analysis Tool, US Department of Transportation Volpe Center, Last Updated March 14, 2014 (https://www.volpe.dot.gov/infrastructure-systems-and-technology/advanced-vehicle-technology/safetyhat-transportation-system)

31. SECY-16-0070, “Integrated Strategy to Modernize the Nuclear Regulatory Commission’s Digital Instrumentation and Control Regulatory Infrastructure,” ADAMS Accession No. ML16126A140

32. SRM-SECY-22-0076, “Staff Requirements – SECY-22-0076 – Expansion of Current Policy on Potential Common-Cause Failures in Digital Instrumentation and Control Systems,” May 25, 2023, ADAMS Accession No. ML23145A181

33. SRM-SECY-93-087, “Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs,” July 21, 1993, ADAMS Accession No. ML003708056

34. Stanley, P. and Arcos Barraquero, V., “STPA Evaluation of Potential Conflicts Between Large Commercial Air Traffic and Small Uncrewed Aircraft Systems in the Terminal Airspace,” MIT STAMP/STPA Workshop, June 2021 (http://psas.scripts.mit.edu/home/wp-content/uploads/2021/06/2021-06-30-1110__Stanley.pdf)

35. STAMP Publications, (http://sunnyday.mit.edu/theses/STAMP-publications-sorted-new.pdf)

36. STPA Handbook, Nancy G. Leveson and John P. Thomas, March 2018

37. Thomas, John, “Investigation of the Use of System-Theoretic Process Analysis at the NRC,” September 2021, ADAMS Accession No. ML22272A315

38. TLR-RES/DE-2022-006, “Hazard Analysis: An Outline of Technical Bases for the Evaluation of Criteria, Methodology, and Results,” June 17, 2022, ADAMS Accession No. ML22172A099

39. Vernacchia, Mark A., “Integration of STPA into GM System Safety Process,” MIT STAMP Workshop, March 27, 2018 (http://psas.scripts.mit.edu/home/wp-content/uploads/2018/04/STPA-Integrated-into-GM-Safety-Process-20feb18-Approved-Rev1.pdf)

APPENDIX A. RELEVANT NRC REGULATORY FRAMEWORK

This Appendix describes the relationship between the process described in this document and the NRC regulatory framework.

Note that the regulations listed below may not necessarily apply to all applicants and licensees. The applicability of the regulatory requirements is determined by the plant-specific licensing basis and any proposed changes to the licensing basis associated with the proposed DI&C system under evaluation.

A.1. 10 CFR 50.54(jj), 10 CFR 50.55a(h)

IEEE 603-1991 or IEEE 279 -1971 as incorporated by reference requires, in part, that components and modules shall be designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with a prescribed quality assurance program.

It is assumed in this document that the HSSSR system is developed in accordance with these regulatory criteria. Pre-scored Systematic Control Methods are techniques and measures that may, in some cases, exceed the current regulatory guidance for meeting these regulatory criteria.

A.2. 10 CFR Part 50, Appendix A, "General Design Criteria (GDC)"

A.2.1. GDC 1, "Quality Standards and Records"

GDC 1, "Quality Standards and Records" – states, in part, that "Structures, systems, and components important to safety shall be designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions to be performed."

Since HSSSR systems are considered of high significance regarding the importance of safety functions to be performed, this GDC applies. It is assumed in this document that the HSSSR system is developed in accordance with these regulatory criteria. Pre-scored Systematic Control Methods are techniques and measures that may, in some cases, exceed the current regulatory guidance for meeting these regulatory criteria.

GDC 1 also states, in part, "Where generally recognized codes and standards are used, they shall be identified and evaluated to determine their applicability, adequacy, and sufficiency and shall be supplemented or modified as necessary to assure a quality product in keeping with the required safety function."

It is assumed in this document that the HSSSR system is developed in accordance with the recognized industry codes and standards. Pre-scored Systematic Control Methods are techniques and measures that may, synthesized from the industry standard IEC 61508 Part 3, normative Annex A which is a recognized safety standard in the petrochemical industry.

GDC 1 also states, in part, "A quality assurance program shall be established and implemented to provide adequate assurance that these structures, systems, and components will satisfactorily perform their safety functions. Appropriate records of the design, fabrication, erection, and testing of structures, systems, and components important to safety shall be maintained by or under the control of the nuclear power unit licensee throughout the life of the unit."

It is assumed in this document that the HSSSR system is developed in accordance with this regulatory criterion.

A.2.2. GDC 13, "Instrumentation and Control"

GDC 13, "Instrumentation and Control," states, "Instrumentation shall be provided to monitor variables and systems over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate safety, including those variables and systems that can affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, and the containment and its associated systems. Appropriate controls shall be provided to maintain these variables and systems within prescribed operating ranges."

The HSSSR system requirements development needs to address the functional requirements stated in this GDC. The Control Methods generated from the EPRI DRAM ensures that HSSSR systematic failures like CCF do not prevent the HSSSR system from performing its safety function.

A.2.3. GDC 19, "Control Room"

GDC 19, "Control Room," states, in part, "Equipment at appropriate locations outside the control room shall be provided (1) with a design capability for prompt hot shutdown of the reactor, including necessary instrumentation and controls to maintain the unit in a safe condition during hot shutdown, and (2) with a potential capability for subsequent cold shutdown of the reactor through the use of suitable procedures."

The scope of NEI 20-07 is HSSSR DI&C systems and these systems need to meet this GDC. The HSSSR system requirements development needs to address the functional requirements stated in this GDC. EPRI HAZCADS and DRAM take into consideration all HSSSR system equipment necessary to perform these functions.

A.2.4. GDC 20, "Protection System Functions"

GDC 20, "Protection System Functions" states, "The protection system shall be designed (1) to initiate automatically the operation of appropriate systems including the reactivity control systems, to assure that specified acceptable fuel design limits are not exceeded as a result of anticipated operational occurrences and (2) to sense accident conditions and to initiate the operation of systems and components important to safety."

The scope of NEI 20-07 is HSSSR DI&C systems and these systems need to meet this GDC. EPRI HAZCADS defines these as control actions, and then analyzes the hazards associated with these control actions when performed in an unsafe manner. EPRI HAZCADS and DRAM also take into consideration inadequate feedback from sensors and control actions that are not executed or not executed properly.

A.2.5. GDC 21, "Protection System Reliability and Testability"

GDC 21, "Protection System Reliability and Testability," states, "The protection system shall be designed for high functional reliability and inservice testability commensurate with the safety functions to be performed. Redundancy and independence designed into the protection system shall be sufficient to assure that (1) no single failure results in loss of the protection function and (2) removal from service of any component or channel does not result in loss of the required minimum redundancy unless the acceptable reliability of operation of the protection system can be otherwise demonstrated. The protection system shall be designed to permit periodic testing of its functioning when the reactor is in operation, including a capability to test channels independently to determine failures and losses of redundancy that may have occurred."

The scope of NEI 20-07 is HSSSR DI&C systems and these systems need to meet this GDC. It is assumed that the HSSSR system must meet the single failure criterion as stated in the GDC. This process assesses HSSSR systematic failures including CCF.

A.2.6. GDC 22, "Protective System Independence"

GDC 22, "Protective System Independence," states in part, "Design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protection function."

The scope of NEI 20-07 is HSSSR DI&C systems and these systems need to meet this GDC. The design basis for operating nuclear plants includes functional diversity for the protective functions. For new plants, the safety analysis for the plant design will develop the necessary functional diversity. EPRI HAZCADS and DRAM evaluate the potential systematic failures of the HSSSR system including CCF. An important aspect of this process is identifying HSSSR systematic misbehaviors in the absence of any HSSSR system faults and failures.

A.2.7. GDC 23, "Protective System Failure Modes"

GDC 23, "Protective System Failure Modes," states, "The protection system shall be designed to fail into a safe state or into a state demonstrated to be acceptable on some other defined basis if conditions such as disconnection of the system, loss of energy (e.g., electric power, instrument air), or postulated adverse environments (e.g., extreme heat or cold, fire, pressure, steam, water, and radiation) are experienced."

The scope of NEI 20-07 is HSSSR DI&C systems and these systems need to meet this GDC. EPRI HAZCADS and DRAM identifies the potential UCAs and the Loss Scenarios that can cause these unsafe control actions. Failing in a safe state is a consideration in the EPRI HAZCADS process.

A.2.8. GDC 24, "Separation of Protection and Control"

GDC 24, "Separation of Protection and Control," states, "The protection system shall be separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel which is common to the control and protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system. Interconnection of the protection and control systems shall be limited to assure that safety is not significantly impaired."

It is assumed in this document that the HSSSR system must meet this regulation. EPRI HAZCADS and DRAM consider all interfaces to the HSSSR system to effectively evaluate the potential systematic failures including CCF.

A.2.9. GDC 25, “Protection System Requirements for Reactivity Control Malfunctions”

GDC 25, “Protection System Requirements for Reactivity Control Malfunctions,” states, “The protection system shall be designed to assure that specified acceptable fuel design limits are not exceeded for any single malfunction of the reactivity control systems, such as accidental withdrawal (not ejection or dropout) of control rods.”

The scope of NEI 20-07 is HSSSR DI&C systems and these systems need to meet this GDC. Not meeting this GDC would be considered a hazard in EPRI HAZCADS and DRAM for assessing the potential HSSSR systematic failures including CCF.

A.2.10. GDC 28, “Reactivity Limits”

GDC 28, “Reactivity Limits” states, “The reactivity control systems shall be designed to have a combined capability, in conjunction with poison addition by the emergency core cooling system, of reliably controlling reactivity changes to assure that under postulated accident conditions and with appropriate margin for stuck rods the capability to cool the core is maintained.”

The scope of NEI 20-07 is HSSSR DI&C systems and these systems need to meet this GDC. Not meeting this GDC would be considered a hazard in EPRI HAZCADS and DRAM for assessing the potential HSSSR systematic failures including CCF.