ALAN CAMPBELL
Technical Advisor, Generation and Suppliers

1201 F Street, NW, Suite 1100
Washington, DC 20004
P: 202.739.8011
adc@nei.org
nei.org

NUCLEAR ENERGY INSTITUTE

April 8, 2022

Mr. Eric J. Benner
Director, Division of Engineering and External Hazards
Office of Nuclear Reactor Regulation
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

Subject: Digital Instrumentation and Control Common Cause Failure Policy Considerations

Project Number: 689

Dear Mr. Eric Benner,

On behalf of the Nuclear Energy Institute's (NEI)[1] members, we provide the attached white paper, "Digital Common Cause Failure Policy Considerations," for NRC staff consideration while addressing a potential expansion to the existing policy documented in SRM/SECY-93-087. The SRM/SECY-93-087 policy was influenced based on the state of digital instrumentation and control technology in the early 1990s. Specific concerns were provided in SECY-91-292 and reaffirmed in SECY-93-087 that led to the use of diversity alone to overcome digital common cause failure. The NRC concerns that contributed to the creation of the SRM/SECY-93-087 policy have been addressed and no longer apply to the technical environment 30 years later. Research has shown that modern analysis techniques (e.g., hazards analysis, reliability analysis, etc.) effectively address digital common cause failure. These techniques are used in non-nuclear industries (e.g., automotive, aviation, chemical processing, and defense industries) in safety critical applications.

Additionally, risk-insights are effective at better informing decisions when addressing digital common cause failure. A risk-informed approach to digital common cause failure allows for the risk significance of individual plant functions to be considered when designing the digital system so that more protection is designed in for those functions of higher risk significance.

Digital I&C technology applications are imperative to the safe and reliable long-term operation of nuclear power plants. This technology is intended to replace obsolete instrumentation and control systems with

[1] The Nuclear Energy Institute (NEI) is responsible for establishing unified policy on behalf of its members relating to matters affecting the nuclear energy industry, including the regulatory aspects of generic operational and technical issues. NEI's members include entities licensed to operate commercial nuclear power plants in the United States, nuclear plant designers, major architect and engineering firms, fuel cycle facilities, nuclear materials licensees, and other organizations involved in the nuclear energy industry.

highly reliable equipment offering improved system functional capabilities (e.g., increased accuracy, no setpoint drift, automation, self-testing and diagnostic capabilities, and data availability to plant staff). The prescribed use of diversity has introduced significant system complexity and cost barriers to replacing the existing systems due to the additional equipment, engineering and maintenance costs associated with implementing diverse systems. Included in the attached white paper, NEI members provide the following recommended principles that should be incorporated into the expanded policy. The new, expanded policy should:

- Allow for risk-informed performance-based approaches to ensure applicants focus on the most risk-significant functions and to provide flexibility in meeting established system performance criteria.
- Consider the full plant defense-in-depth strategy to prevent, mitigate or respond to a digital common cause failure.
- Allow for the use of modern hazards and/or reliability analysis techniques to examine the system for unsafe conditions and identify appropriate system requirements to prevent systematic failures.
- Expand the ability to use design techniques (in addition to diversity) to prevent or mitigate a digital common cause failure in accordance with GDC 22.

The following is an example of an expanded policy based on the considerations detailed above:

1. The applicant shall assess the impact of the proposed digital instrumentation and control Reactor Protection System (RPS) and Engineered Safety Features Actuation System (ESFAS) on the plant's defense-in-depth systems and procedures to demonstrate that vulnerabilities to digital common cause failures have been adequately addressed.
2. In performing the assessment, the vendor or applicant shall identify each digital common cause failure that could adversely impact a safety function using risk-informed hazards and/or reliability analysis techniques.
3. Commensurate with the risk significance of each identified digital common cause failure, the applicant shall demonstrate adequate measures to address the identified digital common cause failure that could adversely impact a safety function. The measures may include non-safety systems or components if they are of sufficient quality to reliably perform the necessary functions and with a documented basis that the measures are unlikely to be subject to the same common cause failure. The measures may also include monitoring and manual operator action to complete a function.

The principles provided are supported by industry research, applied in non-nuclear safety critical applications, and aligned with NRC staff direction to risk-inform regulation where appropriate. Please contact me at adc@nei.org or (202) 439-3698 should you have any questions or concerns.

Sincerely,

Alan Campbell

Attachment: Digital Common Cause Failure Policy Considerations

c: Jeanne Johnston (NRR/DEX/ELTB)
Samir Darbali (NRR/DEX/ELTB)
Bhagwat Jain (NRR/DEX/ESEB)
NRC Document Control Desk

NEI | WHITE PAPER

Digital Common Cause Failure Policy Considerations

Prepared by the Nuclear Energy Institute
April 8, 2022

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.

NEI Project Lead: Alan Campbell

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.

Digital Common Cause Failure Policy Considerations

Common cause failures (CCF) have the potential to introduce failure modes that defeat redundancy. CCF can exist in all systems, including those using analog technology. Traditionally the potential for CCF is minimized through the application of special treatments, such as quality assurance and testing, maintenance, etc. NRC's current policy relative to CCF in digital systems, developed 30 years ago, is unique in that it requires that CCF is assumed to occur, and diversity is the only means of mitigating the failure. The purpose of this white paper is to provide the NRC with information related to a potential expanded policy for digital CCF. The policy considerations described within this document are intended to address digital common cause failure in both Light Water Reactor (LWR) designs, as well as non-LWR designs. Non-LWR designs developing a risk-informed performance-based design and licensing basis use different terminology for terms such as "safety function" and "safety-significant," and have different regulatory requirements.

SRM/SECY-93-087 provides the NRC policy on CCF in digital systems. Within this policy, the NRC provides guidance to:

- assess the defense in depth and diversity of the proposed digital system,
- demonstrate adequate diversity for each postulated common-mode failure (or common cause failure) for each event evaluated in the nuclear power plant's accident analysis,
- provide a diverse means of accomplishing safety functions, if the postulated common-mode failure (or common cause failure) could disable a safety function, and
- provide diverse displays and controls in the main control room for manual, system-level actuation of critical safety functions.

The SRM/SECY-93-087 policy was influenced by NRC staff understanding of the state of digital instrumentation and control technology in the early 1990s. Specific concerns were provided in SECY-91-292 and reaffirmed in SECY-93-087 that led to the use of diversity as the sole means to overcome digital common cause failure. In these SECY papers, the NRC describes the following concerns:

- Lack of digital I&C experience in nuclear applications
- Absence of requirements and standards related to digital-specific design aspects; and
- Lack of guidance and standards related to software development processes.

In the past 30 years, these concerns have been addressed by numerous industries resulting in mature design and software development practices and increased application of digital I&C technology. US and international standards organizations (e.g., Institute of Electrical and Electronics Engineers (IEEE), International Electrotechnical Commission (IEC), and International Society of Automation (ISA)) have developed guidance for the full lifecycle of digital I&C technology and have created robust processes to update these standards. Many of these standards have been endorsed by the NRC for use in nuclear safety-related applications or accepted by NRC in project-specific reviews (e.g., Safety Evaluations for

Triconex[1], RadICS[2], and TXS[3]). Digital I&C technology has been used in numerous nuclear non-safety applications and has been implemented in a limited way within safety-related applications. Many licensees have determined that digital non-safety control system upgrades have significantly decreased turbine-related initiating events. One utility reported that for BWR Digital Feedwater, BWR Turbine Controls, and PWR Turbine Controls upgrades the sites reduced the associated SCRAM rates by 95%, 83%, and 74%, respectively. Outside of the nuclear power generation industry, digital I&C technology is used extensively in safety applications in industries such as automotive, aviation, chemical processing, and defense. As such, risk and hazards analysis techniques have matured to support these safety critical applications. When applied appropriately, modern hazards analysis techniques have been proven effective by researchers and practitioners in identifying systematic failures (including common cause failures). In essence, the NRC concerns that contributed to the creation of the SRM/SECY-93-087 policy 30 years ago have been addressed rigorously in numerous industries and reliance on diversity alone as a means of protecting against common cause failure is no longer needed.

Beyond the SRM/SECY-93-087 policy, diverse systems are not required within 10 CFR Parts 50 and 52. The interpretation of General Design Criterion 22, "Protection system independence," summarized in NUREG-0800 Branch Technical Position (BTP) 7-19 is too narrow. It states that for high safety significant safety-related SSCs, "GDC 22 requires functional diversity, to the extent practical." In fact, GDC 22 states: "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." GDC 22 requires *design techniques* to prevent the loss of the protection function, not *functional diversity*. Limiting design techniques to only functional diversity, as stated in BTP 7-19, or in component (i.e., equipment) design diversity does not fulfill the intent of GDC 22. As a result, no rulemaking would be needed to allow the use of other measures to protect against common cause failure.

In addition, reliance on diversity alone would not reduce the likelihood of a malfunction in the I&C system in all cases. Research of nuclear power plant events concludes that the leading contributing factor to those events was system requirements errors (both I&C and non-I&C system requirements).[4] Implementing diversity may not always be effective in addressing system requirements errors. For example, if the same design requirements are used for the safety system and the diverse system, the same incorrect design functions will be designed into both systems and verified and validated as correct. Additionally, aviation industry experts have identified that system complexity from diverse systems has contributed to errors leading to aircraft accidents.[5][6] Alternatively, modern hazards analysis techniques (e.g., Systems-Theoretic Process Analysis) are effective in the identification of potential design errors that could lead to the failure of system functions. To determine their effectiveness, researchers have provided digital I&C system designs to engineering teams to implement modern hazards analysis techniques.[7] The engineering teams were unaware of defects in these system designs that either led to digital events or were identified in late project stages. Using these modern hazards analysis techniques, the engineering teams successfully identified the design errors earlier in the design process or

[1] "Final Safety Evaluation for the Triconex Topical Report," April 20, 2012. ADAMS Accession Number ML120900899

[2] "Safety Evaluation by the Office of New Reactors and the Office of Nuclear Reactor Regulation AREVA NP Topical Report ANP-10272 Software Program Manual for Teleperm XS Safety Systems," July 5, 2011. ADAMS Accession Number ML111801119

[3] "RadICS Final NONPROPRIETARY SE and Transmittal Letter," July 31, 2019. ADAMS Accession Number ML19134A193

4 EPRI Report 3002005385, "Severe Nuclear Accidents: Lessons Learned for Instrumentation, Control and Human Factors." December 2015

5 Malmquist, Shem, Nuclear Regulatory Commission Regulatory Information Conference, "T7 – Hazard Analysis for Nuclear Automation: Defeating Digital Demons" March 8, 2022

6 Elias, Bart, "Cockpit Automation, Flight Systems Complexity, and Aircraft Certification: Background and Issues for Congress" October 3, 2019. R45939 https://crsreports.congress.gov

7 Thomas, John, "System Integration Approach to Safety-Security" presented at IAEA Technical Meeting on Instrumentation and Control, and Computer Security for Small Modular Reactors and Microreactors, February 24, 2022.

sufficiently addressed the design errors when traditional defense-in-depth and diversity failed to address them effectively.

The use of diversity and modern hazards analysis techniques are not mutually exclusive concepts; rather, these tools are complementary to achieving safe utilization of digital I&C technology. Diversity is an important measure that may be used when implementing digital I&C technology; however, use of diversity should be based on an engineering approach that identifies where diversity is necessary. Additionally, digital common cause failures should not be viewed without the context of the defense-in-depth posture of the plant. All defense-in-depth elements (i.e., plant systems and procedures) should be accounted for in preventing common cause failure and mitigating its effects.

Risk insights applied during digital I&C system development processes lead to better system function allocation between components, better understanding of the impacts of system architectural decisions, and can inform the use of measures to prevent or mitigate a potential common cause failure based upon risk significance. Utilizing risk-informed practices associates specific SSC with their risk significance. In doing so, design techniques to prevent or mitigate digital common cause failure can be informed by the risk-significance allowing engineering, maintenance, and operation teams to improve decision-making based on potential impacts to the nuclear power plant.

Prescribing the use of diversity as the only solution for addressing potential digital common cause failure unnecessarily impedes the use of today's digital I&C technology that can improve safety in nuclear power plants. This technology is intended to replace obsolete instrumentation and control systems with highly reliable equipment offering improved system functional capabilities (e.g., increased accuracy, no setpoint drift, automation, self-testing and diagnostic capabilities, and data availability to plant staff). The prescribed use of diversity introduces unnecessary complexity that has introduced significant system complexity as well as cost barriers to replacing the existing systems due to the additional equipment, engineering and maintenance costs associated with implementing diverse systems. By allowing other methods beyond diversity to address common cause failure will enable the deployment of this safer technology at an accelerated pace.

Based on the information described above, NEI members have developed the following recommendations to be considered in the expansion of common cause failure policy. The new, expanded policy should:

- Allow for risk-informed performance-based approaches to ensure applicants focus on the most risk-significant functions and to provide flexibility in meeting established system performance criteria.

- Consider the full plant defense-in-depth strategy to prevent to the degree practicable, mitigate or respond to a digital common cause failure.

- Allow for the use of modern hazards and/or reliability analysis techniques to examine the system for adverse conditions and identify appropriate system requirements to prevent systematic failures.

- Expand the ability to use design techniques (in addition to diversity) to prevent to the degree practicable or mitigate a digital common cause failure in accordance with GDC 22.

The following is an example of an expanded policy based on the considerations detailed above:

1. The applicant shall assess the impact of the proposed digital instrumentation and control Reactor Protection System (RPS) and Engineered Safety Features Actuation System (ESFAS) on the plant's defense-in-depth systems and procedures to demonstrate that vulnerabilities to digital common cause failures have been adequately addressed.

2. The vendor or applicant shall identify each digital common cause failure that could adversely impact a safety function using risk-insights, and hazards and/or reliability analysis techniques.

3. The applicant shall demonstrate commensurate with the risk significance of each identified digital common cause failure adequate measures to address the identified digital common cause failure that could adversely impact a safety function. The measures may include non-safety systems or components if they are of sufficient quality to reliably perform the necessary functions and with a documented basis that the measures are unlikely to be subject to the same common cause failure. The measures may also include monitoring and manual operator action to complete a function.