IMPACTS OF COMMON CAUSE FAILURE REGULATORY REQUIREMENTS ON PROTECTION SYSTEM ARCHITECTURES

Mark Burzynski
NewClear Day, Inc.
2036 Marina Cove Dr.
Hixson, TN 37343
mjburzynski@newcleardayinc.com

ABSTRACT

Regulatory-based design considerations for potential common cause failures (CCF) in digital instrumentation and control (I&C) systems have evolved over time and have impacted the development of protection system I&C architectures. The single failure criterion used to be the main design driver for a protection system I&C architecture and resulted in the familiar four-fold and three-fold system architectures. The single failure criterion has now been replaced by the conservative assumptions associated with digital CCF concerns (i.e., assumed digital CCF coincident with an anticipated operational transient or postulated accident) which are classified as 'beyond design basis events' by regulatory authorities. It is unusual for a beyond design basis event to be the controlling factor for a safety system design but that is now the reality for I&C system designers. The preferred regulatory solution is to introduce diversity into I&C system designs to guard against the general concern of digital CCF. However, the lack of clear criteria on how to define sufficient diversity (i.e., how much, what kind, and whether it is linked to identified digital CCF vulnerabilities) had led to more complex I&C architectures. The trend has been towards lengthy and more difficult reviews for the treatment of digital CCF vulnerabilities and I&C system architectures because of the subjective definition of digital CCF vulnerabilities and the lack of clear acceptance criteria for diversity strategy. Improvement in the treatment of digital CCF is needed to reverse the trend of increased I&C system architecture complexity and longer regulatory reviews.

Key Words: Digital I&C, NRC review, common cause failure, diversity, system architecture

1 INTRODUCTION

This paper provides a perspective on how the regulatory-based design considerations for potential common cause failures (CCFs) in digital instrumentation and control (I&C) systems have evolved over time and how they have impacted the development of safety system I&C architectures. The discussion will consider what is most important to I&C architecture designs. The evolution of the regulatory criteria will be considered with respect to the resulting impacts on I&C architectures and the associated regulatory design reviews. The discussion focuses on safety-related protection systems, since that is the area with the most review experience; however, the discussion will also look to the future to consider how the regulatory process might impact I&C architectures for lower classified safety systems and non-safety systems.

2 MOST IMPORTANT CRITERION FOR I&C ARCHITECTURE DESIGNS

The single failure criterion has been identified as the oldest and most important requirement in the nuclear industry. It was the main design driver for a protection system I&C architecture and resulted in

the familiar four-fold and three-fold system architectures. The single failure criterion has now been replaced by the conservative assumptions associated with digital CCF concerns (i.e., assumed digital CCF coincident with an anticipated operational transient or postulated accident). These conservative assumptions are classified as 'beyond design basis events' by regulatory authorities. In the nuclear industry, it is unusual for a beyond design basis event to be the controlling factor for a safety system design but that is now the reality for I&C system designers.

The conservative treatment of digital CCF in nuclear I&C first appeared in the US regulatory arena in the early 1990s. The Staff Requirements Memorandum [Reference 1] was issued by the Nuclear Regulatory Commission (NRC) Commissioners in response to SECY 93-087 to provide policy direction for the expected use of highly integrated digital I&C systems in new plant designs. As a result, the NRC has applied the following four-point position on diversity and defense-in-depth for advanced reactors and for digital system modifications to operating plants:

Point 1 - The applicant/licensee should assess the D3 of the proposed I&C system to demonstrate that vulnerabilities to common-cause failures have been adequately addressed.

Point 2 - In performing the assessment, the vendor or applicant/licensee should analyze each postulated common-cause failure for each event that is evaluated in the accident analysis section of the safety analysis report (SAR) using best-estimate or SAR Chapter 15 analysis methods. The vendor or applicant/licensee should demonstrate adequate diversity within the design for each of these events.

Point 3 - If a postulated common-cause failure could disable a safety function, a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common-cause failure, should be required to perform either the same function as the safety system function that is vulnerable to common-cause failure or a different function that provides adequate protection. 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.

Point 4 - A set of displays and controls located in the main control room should be provided for manual system-level actuation of critical safety functions and for monitoring of parameters that support safety functions. The displays and controls should be independent and diverse from the computer-based safety systems identified in Points 1 and 3.

The NRC policy decisions were made based on underlying concerns regarding the use of digital technology in nuclear power plant safety systems presented in SECY-91-292 [Reference 2]. These original concerns were identified as: lack of experience in nuclear applications, evolving technology, absence of requirements and standards related to digital-specific design aspects, and lack of guidance and standards related to software development processes. As such, the preferred approach at the time was to bound the consequences of a digital CCF in a black box manner, since the black box was not well defined due to the issues described in SECY-91-292.

This regulatory approach was applied to the third digital protection system retrofit in the US at the Diablo Canyon Power Plant. The treatment of digital CCF was addressed using bounding consequence analyses that used best-estimate assumptions and methods along with credit for manual operator actions [Reference 3]. This approach to digital CCF did not affect the system architecture. The two earlier digital protection system retrofits did not consider digital CCF in the system design (e.g., Sequoyah Nuclear Plant [Reference 4]).

The conservative guidance was a prudent design approach to be used when digital technology was new and not well understood by the regulatory bodies. Specific design standards applicable to safety aspects of digital technology did not exist at that time. Since then, vendor I&C platform designs and the

regulatory process for digital I&C have evolved on divergent tracks with well-intentioned efforts to address the original concerns with digital CCF. Safety-critical I&C platform designs used for nuclear safety applications and associated design standards have matured and improved (i.e., making I&C systems less vulnerable to a digital CCF). At the same time, regulations associated with the treatment of digital CCF have become more prescriptive (i.e., more digital CCF concerns to consider with more restrictive acceptance criteria). As an example, the use of manual operator actions to mitigate digital CCFs is no longer easy to justify to regulatory authorities and other solutions are generally needed to gain approvals. The preferred regulatory solution is to introduce diversity into I&C system designs to guard against the general concern of digital CCF. However, the lack of clear criteria on how to define sufficient diversity (i.e., how much, what kind, and whether it is linked to identified digital CCF vulnerabilities) has led to more complex I&C architectures.

3 RESULTING IMPACT ON I&C ARCHITECTURES

International Atomic Energy Agency (IAEA) SSG-39 [Reference 5] specifies that "I&C systems should fully meet the requirements of their design basis and unnecessary complexity should be avoided in the design." The experience with digital I&C safety systems has shown that the treatment of digital CCF and associated diversity strategies to address the 'beyond design basis' CCF regulatory criteria have had a significant impact on the complexity of I&C system architectures. Six examples will illustrate the range of impacts on the system I&C architectures and the diversity of solutions. The examples are roughly in chronological order and illustrate the trend towards higher complexity of I&C system architectures. The I&C systems highlighted are all more complex and introduce other design issues that have a nexus to plant safety as the cost for addressing a digital CCF vulnerability. It is important to note that resulting I&C designs address different CCF vulnerabilities: none address all potential CCF vulnerabilities. That is not to suggest that the solutions should (or could) address all digital CCF vulnerabilities. Rather, the point is noted to illustrate that approved solutions address a subset of the digital CCF vulnerabilities; however, the associated diversity acceptance criteria is not clearly linked to relevant or important digital CCF vulnerabilities.

The first example of an I&C system architecture used to address digital CCF vulnerabilities is shown in Figure 1.

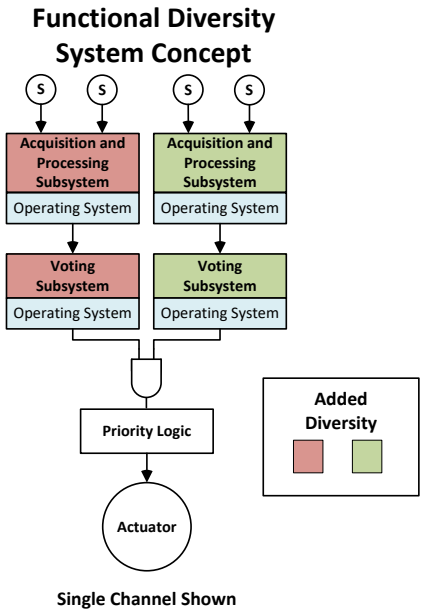

Figure 1. Functional Diversity System Concept

This solution builds on the signal and functional diversity that was present in the original analog system design by using separate functional subsystems [Reference 6, Section 4.2.7]. This addresses CCF vulnerabilities associated with the project-specific application software design; however, the solution does not address CCF vulnerabilities associated with the generic platform operating system.

The Functional Diversity System concept has a small effect on system architecture by allocating the functional diversity to two subsystems using separate application software programs. This results in some increase in hardware to implement the functional diversity in separate subsystems. This solution does not add a separate diverse actuation system and associated system interfaces nor does it rely on additional CCF consequence coping analyses.

The second example of an I&C system architecture used to address digital CCF vulnerabilities is shown in Figure 2.

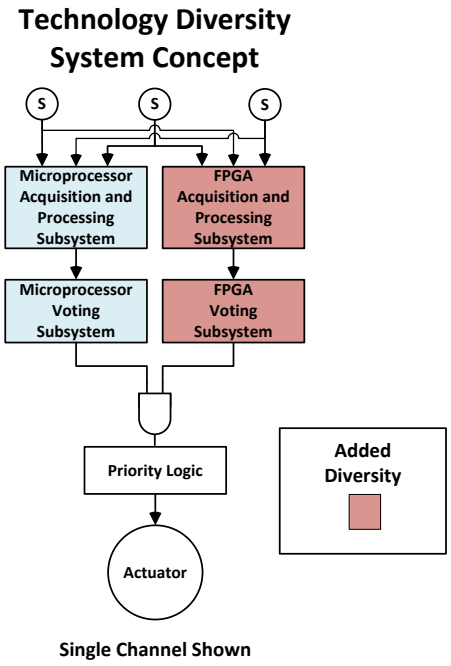

Figure 2. Technology Diversity System Concept

This architecture is an example of mixed (diverse) technology arranged in parallel subsystems and uses field programmable gate array (FPGA) technology as the diversity solution. Other technologies (i.e., digital or analog) could also be used to provide the required diversity.

The Technology Diversity System concept addresses the general CCF vulnerability for a digital technology (i.e., system stops working); however, the solution does not address signal or protection algorithm CCF vulnerabilities.

This solution can be contrasted with the first example. Figure 2 has a greater effect on system architecture by replicating the system functionality in two technology diverse subsystems [Reference 6, Section 4.2.2]. This results in twice the amount of hardware and the additional lifecycle costs to maintain two digital technologies. The Technology Diversity System does not add a separate diverse actuation system and associated system interfaces but it does require coordination of microprocessor and FPGA technologies to understand overall system response times for the different failure scenarios.

This solution can rely on additional CCF consequence coping analyses, since some examples only replicate the reactor trip portion of the protection system while others replicate both the reactor trip and engineered safety feature actuation functions.

The third example of an I&C system architecture used to address digital CCF vulnerabilities is shown in Figure 3.

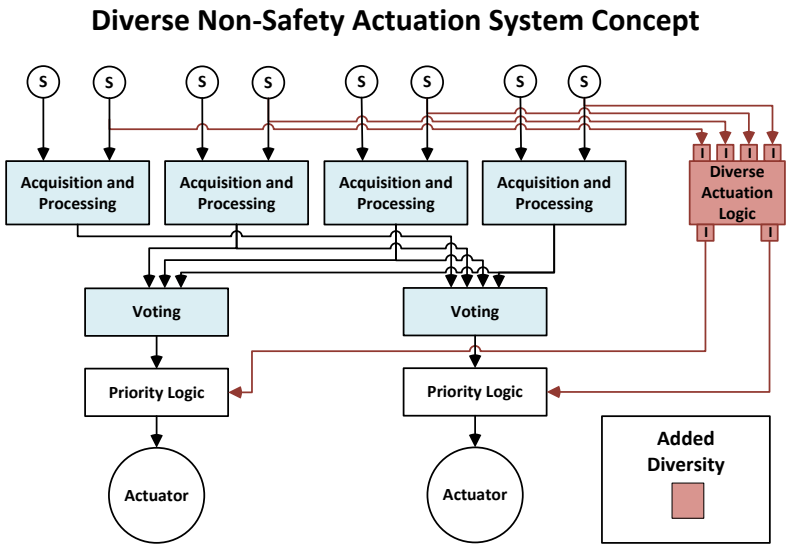

Figure 3. Diverse Non-Safety Actuation System Concept

This solution augments the digital safety system with a small scope non-safety analog actuation system [Reference 7].

This example addresses the general CCF vulnerability for a digital technology (i.e., system stops working); however, it does not address signal or protection algorithm CCF vulnerabilities.

This solution can be contrasted with the first two examples. The Diverse Non-Safety Actuation System concept has a lesser effect on system architecture by only replicating a small portion of the system functionality in the diverse subsystem. This results in some increase in the amount of hardware, as in Figure 1, but it eliminates the additional lifecycle costs to maintain two digital technologies associated with Figure 2.

This example adds additional complexity using a non-safety diverse actuation system and the associated electrical isolation at the interfaces and requires additional design analysis to ensure proper coordination and priority of the non-safety actuation signals. This system also makes the operator tasks more complicated for the non-CCF failure case, since two systems must be reset to let the operator regain control of equipment necessary to support long-term event management or event recovery.

Figure 3 relies on extensive CCF consequence coping analyses to support the small scope of the diverse actuation system.

The fourth example of an I&C system architecture used to address digital CCF vulnerabilities is shown in Figure 4.

FPGA technology has led to other diversity strategies based on internal architecture features to address digital CCF vulnerabilities associated with the electronic design logic development. The solution provided in Figure 4 utilizes two logic cores developed by diverse teams on a single FPGA [Reference 8].

This example addresses FPGA electronic design CCF vulnerabilities but not hardware-related CCF vulnerabilities. The Diverse FPGA Core System concept requires verification of adequate human and design diversity, which must be done after the design solution has been implemented. This diversity approach delays regulatory approval until the implementation phase, which carries a risk of rework late in the development process.

In effect, the concept is a miniaturized version of the design shown in Figure 2. As such, it has a lesser effect on the system architecture but requires additional lifecycle costs to maintain two diverse core designs. Additionally, it does not address signal or protection algorithm CCF vulnerabilities.

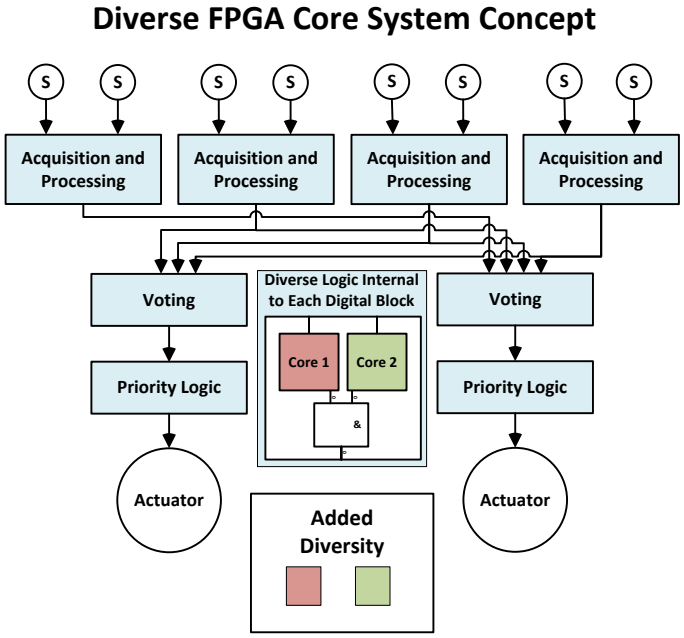

Figure 4. Diverse FPGA Core System Concept

While this system concept does not add a separate diverse actuation system and the associated interfaces, the analysis of the system is more challenging. It requires careful treatment of core output discrepancies to provide clear safe state identification for actuators.

The fifth example of an I&C system architecture used to address digital CCF vulnerabilities is shown in Figure 5.

This solution addresses microprocessor and FPGA electronic design related CCF vulnerabilities. It utilizes the FPGA-based subsystem for a small set of diverse actuation functions that bound the failures of the microprocessor system in a manner like the diverse actuation system shown in Figure 3 [Reference 9].

The Hybrid Diversity System concept addresses the general CCF vulnerability for a digital technology (i.e., system stops working); however, the solution does not address signal or protection algorithm CCF vulnerabilities. Additionally, this system can necessitate verification of adequate human and design diversity in the FPGA-based subsystem in the same manner as described in the previous example.

This solution does not add a separate diverse actuation system and associated interfaces but the analysis of the system is more challenging. Careful treatment of FPGA core output discrepancies is needed to provide clear safe state identification for actuators. Furthermore, this system requires

coordination of microprocessor and FPGA technologies to understand overall system response times for the different failure scenarios.

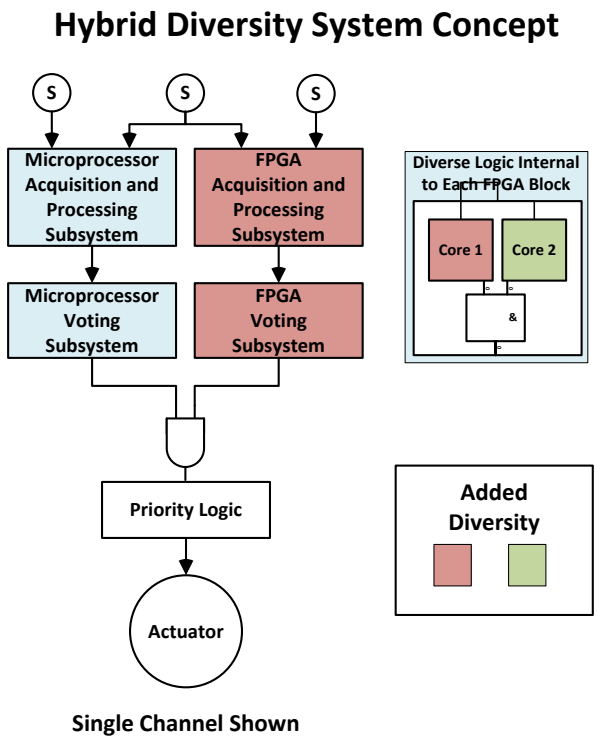

Figure 5. Hybrid Diversity System Concept

Overall, the Hybrid Diversity System concept results in twice the amount of hardware and the corresponding lifecycle costs to maintain two digital technologies, like what was described in example two.

This solution relies on extensive CCF consequence coping analyses to support the limited scope of the FPGA-based subsystem. This system concept was recently used for the replacement of the existing digital protection system at Diablo Canyon. The more complex I&C architecture was chosen to address regulatory concerns with the continued reliance on operator actions to mitigate CCFs coincident with postulated accidents. This experience is an example of how the regulatory treatment of digital CCFs has continued to evolve (i.e., become more prescriptive).

The sixth example, the Diverse FPGA System concept, is shown in Figure 6. Some I&C architectures currently under review by regulatory bodies take advantage of FPGA technology diversity to address chip/electronic design and toolset CCF vulnerabilities [References 10 and 11]. This concept utilizes two subsystems designed with diverse FPGA technology. While Figure 6 addresses FPGA electronic design and hardware related CCF vulnerabilities, it does not address signal or protection algorithm CCF vulnerabilities.

This solution does not add a separate diverse actuation system and associated interfaces. Furthermore, this concept does not rely on additional coping analyses because actuation is provided by the diverse FPGA subsystem in all cases for CCF within an FPGA subsystem.

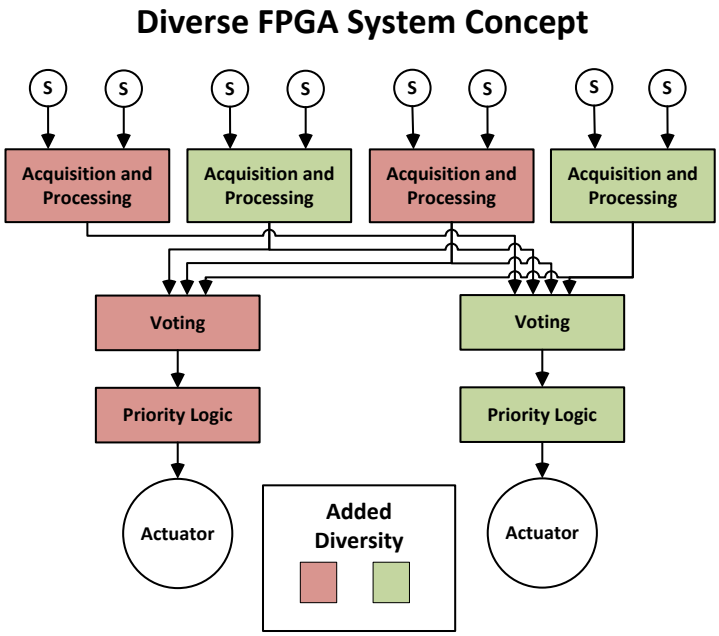

Figure 6. Diverse FPGA System Concept

Ultimately, the Diverse FPGA System concept, if accepted, will return the protection system I&C architecture back to the original (and simpler) architectures used in the analog designs.

4 IMPACT ON I&C ARCHITECTURE REVIEWS

Due to the subjective natures of both the definition of the digital CCF vulnerabilities to be solved and the acceptance criteria for diversity strategies, the timeliness of regulatory reviews has been largely impacted. These factors have also influenced the degree of stability for the regulatory decisions. For example, two popular guidance documents (i.e., NUREG/CR-6303 [Reference 6] and the NUREG/CR-7007 [Reference 12]) focus on addressing a full set of potential diversity attributes with no regard to their relationship or usefulness in mitigating relevant or important digital CCF vulnerabilities. The diversity approach accepted for the Diablo Canyon Eagle 21 systems was not discussed in NUREG/CR-7007.

The trend has been towards lengthy and more difficult reviews of the treatment of digital CCF vulnerabilities and I&C system architectures. These reviews have required more specific and detailed information about the digital review systems to support regulatory decisions. The goals of timely reviews and approvals of I&C architectures early in the system development process expressed in this IAEA document cannot be realized with the current regulatory framework for treatment of digital CCF.

I&C architecture designs would be better if the guidance focused on important CCF vulnerabilities and used appropriate diversity measures to address those vulnerabilities.

5 NEXT I&C ARCHITECTURE CHALLENGE

The preceding discussion has focused on the impacts of regulatory criteria for the treatment of digital CCF vulnerabilities on safety system I&C architectures. Some regulators have raised questions about postulated hazards from non-safety control systems [References 13, 14, and 15]. Their concern is that unanalyzed plant transients may be created. In the extreme case, some regulators have suggested solutions that would prevent a non-safety system network from communicating with actuators for safety

system components. The implications here will affect efforts to improve the man-machine interface (MMI) in the control rooms. It will be necessary to have clear rules on what are credible hazards to consider in plant designs to make practical architecture decisions. Segregation of control elements and between control and MMI networks can be used in non-safety control system architectures to limit effects of hazardous actions attributed to software design errors; however, there is currently no good guidance for applying defensive measures for this design question accepted by all stakeholders.

6 IMPROVED ARCHITECTURE DESIGN PROCESS

As discussed at the beginning of this appendix, vendor I&C platform designs and the regulatory process for digital I&C have evolved on divergent tracks with well-intentioned efforts to address the original concerns with digital CCF. Safety-critical I&C platform designs used for nuclear safety applications and associated design standards have matured and improved (i.e., making I&C systems less vulnerable to a digital CCF). It is important to start convergence of these two tracks to achieve the objectives of timely regulatory approvals of simpler system I&C architectures for nuclear power plant safety systems.

The application of diversity as a panacea for the digital CCF concern has resulted in more complex system architectures with no clear connection between the application of the diversity to the most relevant or important CCF vulnerabilities. The downsides to the added complexity are not routinely considered in the regulatory decisions.

There is now a vast body of operational data from the global deployment of digital I&C in nuclear plants. The safety-critical platforms developed for the global nuclear market have mature design features that provide for deterministic behaviors through the use modern IEC standards. The software development process standards have also matured and are now widely accepted by nuclear regulatory bodies. Mature technology, mature development standards, and modern development and test tools reduce the likelihood of design errors.

It may now be possible to address digital CCF vulnerabilities in the same manner as other topics connected with CCF vulnerabilities (e.g., seismic, environmental, or electromagnetic compatibility). These approaches reduce hazard vulnerabilities to accepted levels using best engineering and design practices rather than trying to make them fully immune. The use of a focused approach in addressing digital CCF vulnerabilities with standardized defensive techniques (e.g., as described in EPRI Report 3002005326 [Reference 16]) may be more effective than specifying degrees of diversity in addressing important digital CCF vulnerabilities or addressing all consequences. These practices could also lead to simpler I&C system architectures.

7 REGULATORY ACTIONS TO ADDRESS DIGITAL CCF

The NRC Commissioners directed their NRC staff to develop an integrated strategy to modernize the digital I&C regulatory infrastructure [Reference 17]. The NRC staff provided their plan to the Commissioners in SECY-16-0070 [Reference 18]. The plan has four specific modernization plans:

MP#1 - Protection against Common Cause Failures
MP#2 - Considering Digital Instrument & Control in Accordance with 10 CFR 50.59
MP#3 - Commercial Grade Dedication of Digital Equipment
MP#4 - Modernization of the Instrument & Control Regulatory Infrastructure

MP#1 addresses the staff evaluation of the NRC's existing positions on defense against CCF. This effort will examine the technical basis to evaluate a graded approach based on safety significance, including consideration of the likelihood of CCF and a risk-informed, consequence based regulatory structure. The objective of assessing the NRC position on potential CCF is to ensure safety and security while enhancing efficiency, clarity, and confidence in determining the potential for CCF in the analysis of

digital I&C systems. This assessment will include examination of state-of-the-art analysis in other digital I&C applications, such as other industries and from other countries.

The NRC Commissioners approved the NRC staff DI&C action plan and added a set of specific follow-up actions [Reference 19]. This approval action indicates that the Commissioners understand the importance of the NRC staff actions to reduce the barriers to I&C modernization with digital technology.

8 CONCLUSIONS

"I&C systems should fully meet the requirements of their design basis and unnecessary complexity should be avoided in the design" (IAEA SSG-39).

The treatment of digital CCF vulnerabilities and their associated diversity strategies have had a significant impact on I&C system architecture design. Improvements to how the regulator approaches digital CCFs are needed to reverse the trends of increased I&C system architecture complexity and longer regulatory reviews.

9 REFERENCES

1. Nuclear Regulatory Commission, "Staff Requirements Memorandum on SECY-93-087, 'Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs'," July 15, 1993. Retrieved from https://www.nrc.gov/reading-rm/adams.html (accession no. ML003708056)
2. Nuclear Regulatory Commission, "Digital Computer Systems for Advanced Light-Water Reactors," SECY-91-292, September 16, 1991. Retrieved from https://www.nrc.gov/reading-rm/adams.html (accession no. ML12222A030)
3. Nuclear Regulatory Commission, "Safety Evaluation Report Eagle 21 Reactor Protection System Modification With Bypass Manifold Elimination, PG&E, Diablo Canyon Power Plant, " October 7, 1993
4. Nuclear Regulatory Commission letter, "Reactor Protection System Upgrades and Enhancements - Sequoyah Nuclear Plant, Unit 2," October 31, 1990
5. International Atomic Energy Agency, "Design of Instrumentation and Control Systems for Nuclear Power Plants," IAEA Safety Standards Series No. SSG-39, IAEA, Vienna (2016).
6. Nuclear Regulatory Commission, "Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems," NUREG/CR-7007, December 2008. Retrieved from https://www.nrc.gov/reading-rm/adams.html (accession no. ML100541256)
7. Duke Energy Corporation letter to NRC, "Oconee Nuclear Station, Units 1, 2, and 3 License Amendment Request for Reactor Protective System/Engineered Safeguards Protective System Digital Upgrade, Technical Specification Change Number 2007-09," January 31, 2008. Retrieved from https://www.nrc.gov/reading-rm/adams.html (accession no. ML080730339)
8. Nuclear Regulatory Commission, "Safety Evaluation for Topical Report 6002-00301 "Advanced Logic System Topical Report," September 2013. Retrieved from https://www.nrc.gov/reading-rm/adams.html (accession no. ML13218A979)
9. Pacific Gas and Electric Company letter DCL-11-104 to NRC, "Diablo Canyon Units 1 and 2 License Amendment Request 11-07 Process Protection System Replacement," October 26, 2011. Retrieved from https://www.nrc.gov/reading-rm/adams.html (accession nos. ML11307A331 and ML11307A332)

10. Lockheed Martin Corporation and State Nuclear Power Automation System Engineering Company, NuPAC_ED610000-047-P, Revision B, “Generic Qualification of the NuPAC Platform for Safety-Related Applications,” January 19, 2012. Retrieved from https://www.nrc.gov/reading-rm/adams.html (accession no. ML13289A270)
11. NuScale Power letter LO-1116-51717 to NRC, “NuScale Power, LLC Submittal of Topical Report TR-1015-18653, ‘Design of the Highly Integrated Protection System Platform,’ Revision 1,” November 4, 2016. Retrieved from https://www.nrc.gov/reading-rm/adams.html (accession no. ML16309A613)
12. Nuclear Regulatory Commission, “Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems,” NUREG/CR-6303, December 1994. Retrieved from https://www.nrc.gov/reading-rm/adams.html (accession no. ML071790509)
13. Nuclear Regulatory Commission, NUREG-0847, Supplement 23, “Safety Evaluation Report Related to the Operation of Watts Bar Nuclear Plant, Unit 2” (Section 7.7.1.4.4.1, Segmentation Analysis), July 2011. Retrieved from https://www.nrc.gov/reading-rm/adams.html (accession no. ML11206A499)
14. Nuclear Regulatory Commission letter to AREVA, “NRC Staff Conclusions on Aspects of the U.S. EPR Digital Instrumentation and Control Systems Design,” July 2, 2013. Retrieved from https://www.nrc.gov/reading-rm/adams.html (accession nos. ML13168A571 and ML13168A603)
15. Korea Electric Power Corporation and Korea Hydro & Nuclear Power Co., Ltd, APR1400-Z-J-NR-14012-NP, Revision 0, “Control System CCF Analysis,” November 2014. Retrieved from https://www.nrc.gov/reading-rm/adams.html (accession no. ML15009A193)
16. Electric Power Research Institute, Technical Report 3002005326, “Methods for Assuring Safety and Dependability when Applying Digital Instrumentation and Control Systems,” 2016.
17. Nuclear Regulatory Commission, “Staff Requirements Memorandum on SECY-15-0106 – Proposed Rule: Incorporation by Reference of Institute of Electrical and Electronics Engineers Standard 603-2009, ‘IEEE Standard Criteria for Safety Systems For Nuclear Power Generating Stations’," February 25, 2016. Retrieved from https://www.nrc.gov/reading-rm/adams.html (accession no. ML16056A614)
18. Nuclear Regulatory Commission, SECY-16-0070, “Integrated Strategy to Modernize the Nuclear Regulatory Commission’s Digital Instrumentation and Control Regulatory Infrastructure,” May 31, 2016. Retrieved from https://www.nrc.gov/reading-rm/adams.html (accession nos. ML16126A140 and ML16097A182)
19. Nuclear Regulatory Commission, “Staff Requirements Memorandum on SECY-16-0070, ‘Integrated Strategy to Modernize the Nuclear Regulatory Commission’s Digital Instrumentation and Control Regulatory Infrastructure’," October 25, 2016. Retrieved from https://www.nrc.gov/reading-rm/adams.html (accession no. ML16299A157)