MODERNIZING APPROCHES TO ADDRESS COMMON CAUSE FAILURE IN DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS

Rossnyev Alvarado and Steven A. Arndt[1]
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555
rossnyev.alvarado@nrc.gov; steven.arndt@nrc.gov

ABSTRACT

As microprocessor-based safety systems were first introduced in nuclear power plants in the US in the 1980s, the U.S. Nuclear Regulatory Commission (NRC) recognized that digital instrumentation and control (DI&C) can provide advantages in reliability and functionality, but that it also creates the potential for a new vulnerability to a common cause failures (CCFs) among systems in which functions are performed by identical software executed in identical hardware. Specifically, the staff recognized that a latent, systemic fault in design or implementation of software could result in the concurrent failure of essential safety or compensating systems. The potential for pervasive and latent systemic faults resulting in a CCF could be more significant for DI&C systems because of increased resource sharing and the potential for unspecified interactions or unanalyzed conditions. In SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," dated April 2, 1993 [1], the NRC staff identified policy, technical, and licensing issues pertaining to evolutionary and advanced light water reactor designs, one of which was defense against CCF in DI&C systems. The staff presented position recommendations for addressing the potential for CCFs in DI&C safety systems. In the Staff Requirements Memorandum (SRM) to SECY SECY-93-087 [2], the Commission approved, in part, and disapproved, in part, the staff's recommendation. The NRC staff implemented the Commission direction into staff guidance for the review of digital I&C systems in a Branch Technical Position (BTP) 7-19, "Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems," [3] in the Standard Review Plan used for new digital systems for new reactors and operating reactors. In the SRM to SECY 16-0070 [4], "Integrated Strategy to Modernize the Nuclear Regulatory Commission's Digital Instrumentation and Control Regulatory Infrastructure", dated October 25, 2016, the Commission approved implementation of the staff's integrated action plan (IAP) to modernize the NRC's digital instrumentation and control regulatory infrastructure. As part the work outlined in the IAP NRC staff has reviewed the current NRC position on defense against CCF in digital I&C systems. This paper outlines the high level principles the staff will be using to update the CCF guidance based on current Commission direction.

Key Words: Common cause failure, software, digital technology, instrumentation and control system, defense-in-depth and diversity

---

[1] This paper was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for any third party's use, or the results of such use, of any information, apparatus, product, or process disclosed in this paper, or represents that its use by such third party would not infringe privately owned rights. The views expressed in this paper are those of the authors and are not necessarily those of the U.S. Nuclear Regulatory Commission.

1 INTRODUCTION

In the Staff Requirements Memorandum (SRM) to SECY 15-0106 [5], the Commission directed the NRC staff to develop an integrated action plan for the modernizing of the instrumentation and control (I&C) regulatory infrastructure. As part of this plan, the staff included the effort to reevaluate the NRC's current position on CCF and measures that can be applied to prevent or mitigate against postulated CCF events.

The current digital I&C licensing and oversight process for power and non-power reactors has been criticized as being cumbersome, inefficient, and/or unpredictable. In particular, industry has suggested the current guidance to perform I&C modification is insufficient regarding: a) how to address the potential for CCF; b) how to acceptably analyze the potential for CCF for its safety impact; and c) and if this analysis will be acceptably used in licensing activities. Additionally, there is a concern that the regulatory treatment and acceptance criteria associated with the analysis of digital I&C systems is too restrictive and costly. This includes concerns associated with how to perform the analysis when considering a modification under the 10 CFR 50.59 process and the scope of the required analysis. Specifically, the current guidance in branch technical position (BTP) 7-19, "Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems" [3], limits the use of design attributes to eliminate CCF from further consideration. BTP 7-19 only identifies two means, simplicity and diversity. The problem with simplicity is that the proper application of "simple systems" is determined by performing 100% testing. Regarding diversity, some applicants interpret this as a requirement to have a separate system, and not considering other type of diversity, such as internal diversity. Although commonly articulated, these are only partly the case. In point of fact a criteria in BTP 7-19 can be meet by a number of different methods include simple systems, internal diversity, manual operator action, previously installed systems (such as anticipated transient without scram (ATWS) mitigation systems) and others. Further, there is a concern that the guidance seems to imply that a full diversity and defense-in-depth (D3) analysis is needed to address vulnerabilities of CCF for all I&C systems, regardless their safety significance. In response to these concerns, NRC staff is considering the recommendations proposed by industry as part of the broader effort to develop a technical basis for evaluating the current NRC position and considering the alternatives available to resolve CCF concerns.

This paper discusses the NRC staff review of CCF in digital I&C using direction provided by the Commission in the SRM to SECY 93-087 [2], while also addressing stakeholders concerns that the current position does not fully recognize the advancements in industry standards and system development processes that have been made in the design of digital systems. In particular the paper will discuss the NRCs efforts to risk inform and grade the analysis needed to demonstrate adequate assurance of protection against CCF, and based on the potential consequences of the CCF, ensure that the required analyses be commensurate with the safety significance of the system.

2 BACKGROUND

Digital Instrumentation and Controls systems have been in use for over three decades in various applications and are systems are widely used in almost all industrial applications in one form or another (e.g., fossil power plants and refineries have been using integrated digital I&C systems since the 1980s). The use of microprocessors and computers is not new in nuclear power plants. However, early applications were limited to programmable logic controllers and plant process monitoring computers. For example, the Core Protection Calculator (CPC) (Digital Safety System) for Combustion Engineer plants was licensed in 1978.

In the 1980s, digital technologies were integrated into control systems for various subsystems, starting with the auxiliary systems and then moving to primary systems. By the 1990s, microprocessors were being used for data logging, control, and display for many non-safety-related functions. But when it came to safety

systems, the NRC staff expressed its concerns about digital safety systems, including potential CCF vulnerabilities.

These concerns were articulated in its SECY 91-292, "Digital Computer Systems for Advanced Light-Water Reactors" [6], and in item II.Q of SECY 93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs" [1]. In SECY 93-087 the NRC staff documented a four-point position on diversity and defense-in-depth that was subsequently modified in the associated SRM, dated July 21, 1993 [2]. CCF of multiple systems (or redundancies within a system) is the main credible threat to defeating the defense-in-depth provisions within I&C system architectures of nuclear power plants (NPPs). It is generally accepted that the unique characteristics and inherent complexity of digital I&C systems can exacerbate this vulnerability [7]. In the SECY 93-087, the staff notes that Electric Power Research Institute (EPRI)'s ALWR requirements document places special emphasis on CCFs to ensure they are addressed in human-machine interface (HMI) system designs. Since EPRI observed that there were no accepted standards at the time to accurately quantify software reliability, the ALWR Program "emphasized the need for software quality and for a defense-in-depth approach to ensure the integrity of I&C functions including requirements for a backup hardwired manual actuation capability for system-level actuation of safety functions." Subsequently, the staff developed potential regulatory guidance for assessing the defenses against CCFs in a digital I&C system design and published it in a draft Commission paper dated June 25, 1992 [6]. The approach proposed by the staff "specified requirements for a backup system which is not based on software and which is used for system-level actuation of critical safety functions and displays of safety parameters."

As discussed in SECY 93-087, the four-point position on diversity and defense-in-depth was generated because hardware design errors, software design errors, and software programming errors are credible sources of CCF for digital safety systems. The safety significance of these potential digital CCFs arises from the prospect that architectural redundancy within a safety system could be defeated and more than one echelon of defense-in-depth could be compromised. The position enhances guidance on addressing the potential for CCF hazards that arise from conventional (i.e., analog) I&C implementations of safety-related functions (e.g., general design criterion (GDC) 22, 10 CFR 50.55a) by addressing the unique characteristics and concerns related to digital technology while remaining consistent with that guidance.

It is noted in SECY 93-087 and SECY 91-292 that quality and diversity are principle factors in defending against CCF vulnerabilities. Criteria for ensuring adequate quality and independence are established in Appendix B of 10 CFR 50 and as part of the design criteria provided in Institute of Electrical and Electronics Engineer (IEEE) Std. 603-1991 [8] and IEEE Std. 7-4.3.2-2003 [9], as endorsed in Regulatory Guide (RG) 1.152 [10]. In SECY 93-087, it is noted that by crediting systems that have previously been classified as non-safety systems, the diversity and defense-in-depth assessment cuts across safety classification for digital I&C systems. Following the establishment of the four-point position in the SRM to SECY 93-087, a branch technical position was developed by the NRC Human Factors and Instrumentations and Control Branch (HICB) to capture guidance on the evaluation of defense-in-depth and diversity for digital computer-based protection systems. This BTP is identified as BTP 7-19 [3].

From the outset of nuclear power development, multiple lines of defense (i.e., defense-in-depth) and diversity have been employed to account for the potential failure of shutdown systems. The Chicago Pile #1 (CP-1) is the first case in which capabilities for defense-in-depth were enhanced by diversity. Thus, defense-in-depth emerged as a fundamental safety principle early in the development of nuclear power. Over the decades, defense-in-depth developed as an approach used by the nuclear power industry to provide progressively compensating systems for facilities with "active" safety systems (e.g., a NPP) in addition to the philosophy of a multiple-barrier approach against fission product release.

Within the protection echelons of defense (i.e., reactor trip system (RTS) and engineered safety features actuation system (ESFAS)), I&C systems are designed to withstand single failures to ensure accomplishment of safety functions even in the presence of random failures. The single failure design

criterion is generally achieved through the implementation of independent, parallel channels or divisions within a safety system in which redundant safety outputs are voted to determine whether to initiate an appropriate safety action. However, redundancy brought with the additional concern of being compromised by a potential CCF. To minimize the potential for CCFs, diversity was the main choice to consider.

3 DETERMINING IF THE NRC POSITION ON CCF NEEDS TO BE UPDATED

Common cause failures are component failures that satisfy four criteria: (1) two or more individual components fail, are degraded (including failures during demand or in-service testing), or have deficiencies that would result in component failures if a demand signal had been received; (2) components fail within a selected period of time such that success of the mission would be uncertain; (3) components fail because of a single shared cause and/or coupling mechanism; and (4) components fail within the established component boundary [7]. It is also important to understand that for instrumentation and control systems used in nuclear power plants, common cause failure are not cascading failures or failures that cause consequential component, module or channel failures. For instrumentation and control systems in nuclear power plants these failures are defined by regulation (10 code of federal regulation (CFR) 50.55(a)(h) as single failures even though they may meet the definition above. Single failures included cascading failures are required to meet different design requirements.

CCF events are not limited to digital systems. Early in the establishment of nuclear safety oversight, the Advisory Committee on Reactor Safeguards (ACRS) stated that the applicant and the Atomic Energy Commission (AEC) regulatory staff should review the proposed designs for common cause failures (identified as common-mode failures (CMFs) at the time), taking into account the possibility of systematic, non-random, concurrent failures of redundant devices, which was not considered in the single-failure criterion (SFC). All through the 1970s and 1980s the ACRS considered improvements and recommendations in the design of systems that would reduce the possibility of CCFs. To address this, the NRC developed the defense-in-depth guidelines to supplement the existing regulatory requirements (single failure criterion, etc.) for protection of the plant. That is, this defense-in-depth analysis was in addition to the evaluation of conformance to all other requirements for reactor protection systems. Specifically, three echelons were identified so that failures in equipment and mistakes by people would be covered such that the public health and safety would be preserved in spite of failures.

With the introduction of digital technology, the concern focus on the different hazards that this technology present when used to support the safe operation of Nuclear Power Plants. When microprocessor-based safety systems were first introduced in the 1980s, the nuclear power industry recognized the prospect for significant CCF vulnerability among digital systems in which identical software is executed on identical hardware. The concern is that a latent, systematic fault in the design or implementation could be present in all identical systems and result in the concurrent failure of essential safety or compensating systems during a demand. Furthermore, the potential safety impact of latent systemic faults resulting in a CCF could increase for digital instrumentation and control systems that incorporate resource sharing or that do not adequately specify and constrain interactions.

As discussed above, the NRC position on CCF is described in SRM-SECY-93-087. This position indicates that digital systems are susceptible to CCF. Nonetheless, NRC position and guidance recognize that there are means to address this vulnerability to eliminate it from further consideration. As mentioned before, BTP 7-19 provides guidance on the evaluation of defense-in-depth and diversity for digital computer-based protection systems. Specifically, this BTP provides the criteria for assessing adequate diversity (which is based on the four-point position from the SRM to SECY 93-087). The BTP states that high quality, defense-in-depth, and diversity are key elements in digital system design. The assessment method documented in NUREG/CR-6303, “Methods for performing Diversity and Defense-in-Depth

Analyses of Reactor Protection Systems" [11], is cited as acceptable for demonstrating that vulnerabilities to CCFs have been adequately addressed in all of the revisions to BTP 7-19.

This situation has led to a great deal of confusion among licensees and the NRC staff and uncertainty regarding the licensing requirements for adequately addressing D3 matters. There have also been misinterpretations of the guidance that have led to situations in which CCF has not been appropriately address under 50.59 modification, which has led to adverse inspection findings.

To resolve this, NRC staff evaluated its current position to determine if it remains adequate, requires modification, or even replacement. NRC staff considered operating experience and research associated with the analysis of digital system failures [12], including evolution of digital system design and implementation, digital system failures continue to occur. The staff found that significant progress has been made in improving the design processes and methods, which would ultimately reduce the likelihood of a failure due to a CCF. For example, high quality design processes detect and correct many implementation errors. Nonetheless, complete elimination of all vulnerabilities of I&C systems and architecture to common cause failure is not achievable. Therefore, the current question is focusing on determining the acceptable means for addressing digital CCF to ensure the plant continues to maintain adequate defense against CCF vulnerabilities.. Different design techniques can be used to address different categories of failures, and some can be used to eliminate the failure from further consideration. This translates to accepting the plausibility of a software CCF, but emphasizing in the methods to minimize such an occurrence and address or cope with such event.

The authors believes that the Commission high level direction in SRM to SECY 93-087 remains appropriate and sufficiently flexible to provide additional regulatory changes that support digital I&C implementation. This is summarized in SECY-18-0090 [13]. This information SECY also describes the plan to update and clarify guidance associated with evaluating and addressing potential CCF of DI&C systems.

4 DEVELOPMENT OF UPDATED GUIDING PRECIPLES

Since the potential for CCF constitutes a credible threat to system operation, the vulnerabilities of a system to failures due to CCF should be evaluated. BTP 7-19 provides an approach to perform a diversity and defense-in-depth analysis to demonstrate adequate protection against CCFs that could disable a safety function for all design basis events identified in Chapter 15 of the Safety Analysis Report (SAR).

This guidance acknowledges that mitigating measures can be employed to moderate or alleviate the effect of an event or to reduce the probability of the occurrence of the event. Mitigation of CCF implies fault tolerance at a safety function level rather than at a particular system level. The guidance in BTP 7-19 identifies two mitigating measures to eliminate CCF from further consideration. One is to use diversity, the other is testability. In the NRC's current position, diversity is specified as a defense against postulated CCF that could disable a safety function. In this case, it is assumed that if a diverse system is used, a failure in one system will not necessarily imply a failure in the other system. Testability was identified in the interim staff guidance (ISG)-02 [14] as a sufficient design attribute to eliminate consideration of CCF. After this ISG was sunsetted, the guidance was incorporated into BTP 7-19.

In addition, the NRC's expectations for defense-in-depth and diversity are embodied in various regulatory requirements. An analysis is expected to determine whether safety functions are vulnerable to common cause failure, and if so, to identify diverse manual or automatic means that can perform the same or different functions in order to mitigate design basis accidents and transients. With this in mind, the staff is working on updating its guidance for clear implementation of NRC's position.

Stakeholders identified that their highest priority is to be able to implement I&C modifications under 10 CFR 50.59, "Changes, Test and Experiments," with no prior NRC staff review and approval. 10 CFR 50.59 is an important aspect of any system modifications and replacement of existing equipment. Since virtually all U.S. nuclear plants have original analog equipment, 10 CFR 50.59 is of particular interest if a licensee is contemplating a digital modification or upgrade. To help licensees, the NRC staff's effort focused on providing clarity of mutual industry and staff understanding that NRC guidance is being properly translated into industry actions for performing 10 CFR 50.59 evaluations of proposed digital I&C plant modifications. Specifically, the NRC issued Regulatory Issue Summary (RIS) 2002-22, Supplement 1 [15]. In the original RIS in 2002 [16], the NRC endorsed licensing and technical guidance provided in Nuclear Energy Institute (NEI) 01-01 [17] for making digital upgrades using 10 CFR 50.59. NEI 01-01 provides guidance for defense-in-depth and diversity (D3) and notes that a D3 analysis per BTP 7-19 Revision 4 is expected only for substantial digital replacements to RTS and ESFAS. This RIS supplement clarifies the staff's endorsement for use of NEI 01-01 and provides a clarification of staff guidance for using a qualitative assessment for determining that CCF is sufficiently low, within the context of qualitative findings that can be made for 10 CFR 50.59 for safety systems other than RTS and ESFAS. It is important to note that the supplement is to support modifications of systems of lower safety significance, such as auxiliary safety support systems, and it does not address major upgrades to RTS and ESFAS.

The next priority was to provide clarifying guidance associated with evaluating and addressing potential CCF of DI&C systems in future licensing actions. Stakeholders have indicated that identifying how to address vulnerabilities to CCF is high-priority, and this is also required for resolution of many others issues related to digital systems regulatory issue. In SECY-18-0090, the staff identified several guiding principles that will facilitate this task. These principles are abridged as follows:

- Evaluate and address CCF due to software for digital systems.
- A D3 analysis should be performed to demonstrate that vulnerabilities to a CCF have been identified and adequately addressed. The D3 analysis should be commensurate with the safety significance of the system.
- If a postulated CCF could disable a safety function, then a diverse means, not subject to the same CCF, should perform either the same function or a different function.
- Technical justification should be provided to demonstrate that defensive measures are adequate to address potential CCFs.

These proposed guiding principles are meant to ensure consistent application of the Commission's direction in SRM to SECY 93-087, and they will be used to clarify the evaluation criteria for addressing vulnerabilities to common cause failure.

In May 2018, the NRC issued Supplement 1 to the RIS 2002-22 to address challenges with replacement using section 50.59 of auxiliary safety support systems, non-safety systems, and individual components. This supplement provides additional clarification on the key technical decision in determining whether the likelihood of common cause failure is sufficiently low, by providing clarifying guidance as to how one may use a qualitative assessment to make this determination, after having first performed an adequate failure modes and effects analysis, a defense in depth analysis, and adhered to appropriate quality processes.

The Supplement 1 to RIS 2002-22 is consistent with these guiding principles. For example, the use of a graded analysis and documentation in relationship to system safety significance is consistent with the approach described in the RIS. Further, the use of a graded approach would be consistent with the agency-wide efforts of implementing a risk-informed regulatory approach.

Regarding the use of the Supplement 1 to RIS 2002-22, failure analysis can be used to identify possible CCF vulnerabilities and assess the need to further modify the design. In some cases, design features and attributes could be used to preclude potential failures from further consideration. Modifications that use

design attributes and features such as internal diversity or segmentation help to minimize the potential for CCFs. The goal of this guidance is to address careful consideration and translation of design requirements into hardware/software requirements, and the application of simple design attributes like performing a segmentation analysis when designing networks, design for elimination of possible concurrent triggers, use of hardware-enforced unidirectional communications, use of redundant controllers in a master/slave arrangement, use of internal or external diversity, watchdogs that are independent of software, use of highly-testable components, use of redundant networks, and others. Such design attributes could serve to prevent, limit, or mitigate the consequences of CCFs.

The staff plans to update BTP 7-19 to include these guiding principles. BTP 7-19, which provides guidance to implement the Commission's direction for licensing actions. Specifically, this BTP provides guidance for performing diversity and defense-in-depth analyses to demonstrate that vulnerabilities to common cause failure are addressed. Regarding these guiding principles, the staff will be included to clarify the level of a D3 analysis to be performed for safety systems. Stakeholders have questioned the necessity of applying guidance on a defense-in-depth and diversity analysis to safety-related auxiliary support systems and non-safety systems. Thus, the staff will develop a graded approach commensurate with the safety significance of the system. For safety and protection systems (i.e., RTS or ESFAS) and systems whose failure could prevent a required safety function credited in the plant safety analyses from being accomplished, the potential consequences of a common cause failure due to software defects can be significant enough (e.g., preventing all redundant protection channels from functioning) to warrant special treatment of the design, in which case a D3 analysis should be performed to demonstrate that vulnerabilities to CCF have been addressed. In performing this analysis, the licensee should analyze each postulated CCF for each event evaluated in the accident analysis section of the safety analysis report.

For other safety systems, such as other than protection systems, especially safety systems that are designed to be functional in redundant trains, whose failure could also prevent important safety functions credited in the SAR from being accomplished (e.g., redundant safety heating, ventilation, and air conditioning (HVAC) systems/chillers, essential cooling water systems, emergency diesel generator trains, etc.) the analysis may be very simple if the digital upgrade is not implemented at a level that impacts the defense-in-depth of the plant. In this case a demonstration via formal design basis methods or a simplified analysis using beyond-design-basis methods (realistic assumptions, conditions) that either sufficient diversity exists in the design of the system, or that preventative or mitigative measures have been included in the design, and/or that alternate means of coping with the failure are available and the results of any new malfunctions are bounded within design basis analyses would be sufficient.

For example, for replacement of safety systems of low significance, such as the HVAC system, which is safety significant, albeit low when compared to RTS and ESFAS, the level of D3 analysis rigor and details for the chiller controls would be less when compared to that required by the RPS and ESFAS. In this case, the concern is whether a common cause failure in the chiller controls needs to be addressed as this system maintains safety related equipment below the plant's environmental qualification limit. Thus, the D3 analysis could simply consist of demonstrating that there is adequate indication of a chiller controls failure and that there is adequate time for plant operators to respond to their failure (by bringing fans to the control room). The Supplement 1 to the RIS 2002-22 provides guidance on how to document this evaluation.

Note that CCF events are of concern to both safety-related and non-safety systems. For non-safety systems, licensees are performing more aggregation of control functions onto a single digital platform and/or use of a common network linking several digital platform to preform different control functions. A common cause failure of these systems could lead to new types of accidents or malfunctions not previously evaluated in the current plant's SAR. Because of staff's concern on this regard, this has caused confusion to the licensee which has created the misunderstanding that the NRC requires the postulation of a CCF and subsequent D3 analysis for all section 50.59 upgrades, which will therefore make it unable to pass the criteria. In this case, the revision to BTP 7-19 will clarify that the NRC's position is that any potential common cause failure in safety and non-safety systems that could impede the performance of a safety

function or result in a plant condition that cannot be mitigated needs to be addressed. For example, for replacement of a non-safety system, the level of D3 analysis (which could rely on a failure analysis that identifies CCF vulnerabilities) rigor would be less due to its lower safety significance when compared to analysis and rigor for RTS and ESFAS. Thus, the D3 analysis could simply consist of demonstrating that the system failure is bounded by the SAR design basis analysis.

Finally, the NRC staff will develop and include guidance for using effective qualitative assessments of the likelihood of failures and use of defensive measures for eliminating CCF from further consideration in its update to BTP 7-19. Industry has proposed using defensive measures to design digital safety systems make them less susceptible to CCFs and/or better able to cope with CCFs should they occur. In particular, the staff will develop guidance to identify defensive measures that could be used to reduce the likelihood of CCFs. This guidance will be consistent with the approach described in the Supplement 1 to the RIS 2002-22, which consider the following factors: (1) the design attributes of the system; (2) quality of the design process; and (3) any relevant operating history with the proposed system.

In addition, the staff will resolve comments provided by stakeholders, including industry, on the current version of BTP 7-19; in particular to clarify the scope of applicability, consideration of design features to eliminate common cause failure from further consideration, and the overall need for diverse actuation systems in some systems in which common cause failure may be a significant vulnerability.

As the staff address broader modernization activities, the staff will address common cause failure technical and regulatory challenges as appropriate. Furthermore, the staff is performing a strategic assessment to identify impactful improvement activities consistent with the Commission direction in SRM-15-0106 [5] and associated recommendations by the Transformation Team in SECY-18-0060, "Achieving Modern Risk-Informed Regulation," [18], which includes potential alternatives to the currently endorses standards. Nonetheless, the staff will continue to consider the challenges and potential impediments that may be unique to specific DI&C as digital technologies and reactor designs continue to evolve.

5 CONCLUSIONS

The authors believes that that the Commission's direction in SRM-SECY-93-087 addresses CCF in digital l&C systems and provides adequate flexibility for regulatory modernization activities that support near-term Dl&C implementation.. To ensure consistent application of the NRC's position on defense against CCF in current and future DI&C system designs, guidance is being updated using the guiding principles described in this paper. Nevertheless, the NRC staff may re-evaluate the Commission position based on long term research, improvements in the state of knowledge of software, and new I&C architectures used for advanced reactor designs.

The staff will continue to engage the industry and other external stakeholders through the DI&C Steering Committee and established regulatory processes to provide an effective path forward to improve the digital I&C review process.

6 ACKNOWLEDGMENTS

The authors wish to acknowledge the work to all of the NRC staff that have contributed to the the IAP and its activities including those discussed in this paper.

7 REFERENCES

1. SECY-93-087, “Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs,” U.S. Nuclear Regulatory Commission, Washington, D.C, 1993.
2. SRM to SECY 93-087, “Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs,” U.S. Nuclear Regulatory Commission, Washington, D.C, 1993.
3. Branch Technical Position (BTP) 7-19, “Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems,” revision 7, U.S. Nuclear Regulatory Commission, Washington, D.C., 2016.
4. SRM to SECY-16-0070, “Integrated Strategy to Modernize the Nuclear Regulatory Commission’s Digital Instrumentation and Control Regulatory Infrastructure,” U.S. Nuclear Regulatory Commission, Washington, D.C, 2016.
5. SRM to SECY 15-0106, “Rulemaking: 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,” U.S. Nuclear Regulatory Commission, Washington, D.C., 2015.
6. SECY 91-292, “Digital Computer Systems for Advanced Light-Water Reactors,” U.S. Nuclear Regulatory Commission, Washington, D.C., 1991.
7. NUREG/CR-6268, “Common-Cause Failure Database and Analysis System: Event Data Collection, Classification, and Coding,” revision 1, U.S. Nuclear Regulatory Commission, Washington, D.C, 2007.
8. IEEE 603-1991, “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations,” 1991.
9. IEEE 7-4.3.2-2003, “IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations,” 2003.
10. Regulatory Guide 1.152, Criteria for Use of Computers in Safety Systems of Nuclear Power Plants,” revision 3, U.S. Nuclear Regulatory Commission, Washington, D.C, 2016,
11. NUREG/CR-6303, “Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems,” U.S. Nuclear Regulatory Commission, Washington, D.C, 1994.
12. S.A. Arndt, R. Alvarado, B. Dittman, Kenneth Mott and R.T. Wood, “NRC Technical Basis for Evaluation of Its Position on Protection Against Common Cause Failure in Digital Systems Used in Nuclear Power Plants,” *Proceedings of the 10th ANS International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies*, June 2017.
13. SECY-18-0090, “Plan for Addressing Potential Common Cause Failure in Digital Instrumentation and Control,” U.S. Nuclear Regulatory Commission, Washington, D.C, 2018.
14. Interim Staff Guidance (ISG)-02, “Diversity and Defense-in-Depth Issues,” revision 2, U.S. Nuclear Regulatory Commission, Washington, D.C, 2009.
15. NRC Regulatory Issue Summary 2002-22, Supplement 1, Clarification on Endorsement of Nuclear Energy Institute Guidance in Designing Digital Upgrades in Instrumentation and Control Systems,” U.S. Nuclear Regulatory Commission, Washington, D.C, 2018.

16. RIS 2002-22, “Guideline On Licensing Digital Upgrades: EPRI TR-102348, Revision 1, NE I01-01: A Revision of EPRI TR-102348 To Reflect Changes to the 10 CFR 50.59 Rule,” U.S. Nuclear Regulatory Commission, Washington, D.C, 2002.
17. Nuclear Energy Institute (NEI) 01-01, NRC Regulatory Issue Summary on EPRI Digital Licensing Guideline, TR-102348,” Nuclear Energy Institute, 2004.
18. SECY-18-0060, “Achieving Modern Risk-Informed Regulation,” U.S. Nuclear Regulatory Commission, Washington, D.C, 2018.