NRC TECHNICAL BASIS FOR EVALUATION OF ITS POSITION ON PROTECTION AGAINST COMMON CAUSE FAILURE IN DIGITAL SYSTEMS USED IN NUCLEAR POWER PLANTS

Steven A. Arndt, Rossnyev Alvarado, Bernard Dittman and Kenneth Mott[1]
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555
steven.arndt@nrc.gov; rossnyev.alvarado@nrc.gov; bernard.dittmand@nrc.gov;
kenneth.mott@nrc.gov

Richard Wood
Department of Nuclear Engineering
University of Tennessee
Knoxville, TN 37996
rwood11@utk.edu

ABSTRACT

Digital technology has advantages over analog systems, including automated monitoring and alerts for standby safety functions, and predictive algorithms to maintain critical safety systems. Additionally, digital technology generally has higher reliability and can be designed to reduce single point vulnerabilities. For these reasons many nuclear plants have applied digital technology to safety and non-safety related applications, including reactor protection system, feedwater and turbine controls, etc. with a corresponding significant improvement in trip reduction. Nonetheless, digital instrumentation and control (I&C) systems also present potential new vulnerabilities that need to be assessed, including potential failures due to increased complexity of digital systems, the introduction of unique failure modes due to software (including software common cause failure (CCF)), and limited operating history of digital systems in nuclear safety related applications compared to analog systems. The fact that software is intangible means that common methods, such as analysis or testing, used for detecting CCF may not be effective when applied to software. Consequently, digital technology is perceived to pose a potential risk from the introduction of undetected systematic faults that could result in CCF. Despite the I&C system upgrades and modifications performed to date, the U.S. Nuclear Regulatory Commission (NRC) and industry stakeholders have identified the need to modernize the regulatory infrastructure to efficiently address risks associated with the use of digital technology for nuclear safety applications and address regulatory uncertainties. The NRC's current position on CCF is guided by the staff requirements memorandum (SRM) on SECY 93-087. The SRM provides specific acceptance criteria for the evaluation of CCF, which the staff implemented in the Branch Technical Position (BTP) 7-19. However, industry stakeholders have proposed using methods to characterize the likelihood of software CCF and eliminate it from further consideration in a defense-in-depth and diversity analysis. The NRC's current position does not consider these alternatives, and thus corresponding acceptance criteria is not currently available. The work discussed in this paper assesses the underlying technical basis associated with CCF, provides technical support for updating the NRC

[1] Although this paper reports on efforts by staff of the U.S. Nuclear Regulatory Commission (NRC), the information and views expressed in the paper are those of the authors and are not necessarily those of the NRC. Neither the U.S. Government nor any agency thereof, nor any of their employees, make any warranty, expressed or implied, or assumes any legal liability or responsibility for any third party's use.

position and considers proposed methods for addressing potential CCF in digital systems while enhancing efficiency, clarity, and confidence.

Key Words: Common Cause Failure, Software, Digital technology, Instrumentation and Control system, defense-in-depth and diversity

1 INTRODUCTION

In 2014 the U.S. Nuclear Regulatory Commission (NRC) started a project to reevaluate its current position on common cause failure (CCF) of digital systems. Then, in the Staff Requirements Memorandum (SRM) to SECY 15-0106 [1], 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.

Representatives of the nuclear industry have stated that the current digital I&C licensing and oversight process for power and non-power reactors is cumbersome, inefficient, and/or unpredictable. In particular, they have suggested the current guidance to perform I&C modification has insufficient details regarding: a) how to address the potential for CCF; b) how to acceptably analyze the potential for CCF for its safety impact; and c) how this analysis may be acceptably used in licensing activities. Further, licensees have stated that the current regulatory treatment and acceptance criteria dealing with the potential for CCF in the analysis of digital I&C systems has been problematic and 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" [2], limits the use of design attributes to eliminate CCF from further consideration. Specifically, they have stated that the proper application of the criteria in BTP 7-19 for "simple systems" in the staff's review guidance, and the lack of a graded approach based on safety significance for CCF analysis are challenges to the licensing of digital systems and need to be evaluated. The 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 provides a summary of some of the information developed to date in support of the effort currently underway by the NRC staff to examine the state-of-the-art for the design and development of digital I&C systems for nuclear power plant (NPP) applications and examines approaches used in other digital I&C applications, such as other industries and other countries. The effort will examine the technical basis for concerns with CCF in digital systems and what they may indicate about the need to reaffirm or revise the current NRC position on CCF in digital systems.

2 REGULATORY BACKGROUND

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. In 1956, Atomic Energy Commission (AEC) Chairman Libby, in response to questions from Senator Hickenlooper, discussed the principle of defense-in-depth. The defense-in-depth principle was advanced mainly in response to the anticipation that degradation may not be wholly predictable and that safety can be best assured by multiple lines of defense. 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 commercial NPP) in addition to the philosophy of a multiple-barrier approach against fission product release.

Early in the establishment of nuclear safety oversight, the Advisory Committee on Reactor Safeguards (ACRS) noted its concerns about using signals from the protection system for control and override purposes. The Committee's belief was that control and protection instrumentation should be as nearly independent as possible, so that the protection will not be impaired by the same fault that initiates a transient requiring protection. The ACRS further stated that the applicant and the 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. However two generic issues required additional technical evaluations. These two items were Anticipated Transients without Scram (ATWS) and CCF.

In 1979, the NRC evaluated in its NUREG-0493, "A Defense-in-Depth and Diversity Assessment of the RESAR-414 Integrated Protection System [3]," the design bases and functional approach given by Westinghouse for analyzing computer-based reactor protection systems and found the potential for design vulnerabilities to common-mode failure. This NUREG explicitly developed the defense-in-depth guidelines that supplemented the existing requirements (single failure criterion, etc.) rather than to replace them. 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. This NUREG also considers the possibility of causal failure of two or more echelons of defense. NUREG-0493 addressed this problem by introducing the concept of dividing the instrumentation systems into blocks as a systematic way to evaluate the defense-in-depth of a design. To conduct a defense-in-depth analysis, components of the system architecture had to be defined.

At that time NUREG-0493 was an assessment of a single reactor protection system that addressed CMF concerns and introduced a method of analysis. Interdependence between reactor trip and engineered safety features (ESF) was outside the scope of the review in NUREG-0493 because this was identical to the ATWS issue that was being treated as a separate generic issue. Although the application of NUREG-0493 was specific to the RESAR-414, the 1979 work established sufficiently general principles that it was adapted to analyze the GE ABWR in 1991, the Westinghouse AP-600 in 1993, and the GE SBWR in 1993. ABB Combustion Engineering used the principles themselves in 1992 to analyze their System 80+ protection system. NUREG-0493 was rewritten in 1994 to describe techniques to determine points of vulnerability in a design to common-mode failures, should they occur. The 1994 version considered the Commission directions provided in SRM to SECY-93-087 [4]. In 1984, the ATWS issue was resolved with the issuance of the ATWS rule (10 CFR 50.62). The final rule requires diverse equipment to mitigate the consequence of an ATWS. Specifically, the ATWS mitigation system must automatically initiate the auxiliary (or emergency) feedwater system and initiate a turbine trip under conditions indicative of an ATWS. However, resolution of CCF issue has not resulted in rule-making, but warranted consideration of additional diversity usage. In the early 1990s, the NRC began reviewing advanced reactor designs developed by General Electric, Combustion Engineering, and Westinghouse. Questions included whether it would ever be possible to estimate the probability of common faults and other design flaws leading to software failure that could impact reactor safety. A study panel constituted by the National Academies of Science and Engineering found that common-cause software failures were credible, and it recommended maintaining diversity in digital safety systems using robust techniques [5].

The NRC staff expressed its concerns about digital safety systems, including potential CCF vulnerabilities, 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" [7]. In SECY 93-087 the NRC staff documented a four-point position on diversity and defense-in-depth (D3) that was subsequently modified in the associated SRM, dated July 21, 1993 [4]. The potential for CCF of multiple systems (or redundancies within a system) constituted the principle credible threat to defeating the defense-in-depth provisions within I&C system architectures of NPPs. It is generally accepted that the unique characteristics and inherent complexity of digital I&C systems can exacerbate this vulnerability [5].

In the SECY (93-087), the staff notes that EPRI's advanced light-water reactor (ALWR) requirements document [8] 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. 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 vulnerabilities that arise from conventional (i.e., analog) I&C implementations of safety-related functions (e.g., general design criterion (GDC) 22, 10 CFR 50.62) 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 IEEE Std 603-1991 [9] and IEEE Std 7-4.3.2-2003 [10], as endorsed in Regulatory Guide 1.152 [11]. 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 (BTP) 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 [2].

BTP 7-19 provides guidance for review of defense-in-depth and diversity (D-in-D&D) assessments and the design of manual displays and control. 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" [12], is cited as acceptable for demonstrating that vulnerabilities to CCFs have been adequately addressed in all of the revisions to BTP 7-19.

In November 2006, industry representatives stated that there was confusion or insufficient guidance addressing digital I&C (DI&C) technology so additional guidance was needed to provide for improved licensing certainty for new plants. In early 2007, NRC formed a steering committee to lead the effort in addressing issues associated with the application of computer-based DI&C systems in safety systems at NPPs. One outcome of this effort was the issuance of Interim Staff Guidance (ISG) DI&C-ISG-02, "Diversity and Defense-in-Depth (D3) Issues" [13], which provided guidance and positions that addressed problem statements identified in cooperation with the industry.

One of the issues addressed by DI&C-ISG-02 is the acceptability of manual actions to fulfill the need for diverse means of accomplishing a backup safety function. This was later revised to state that an automated system is the preferred method for providing an independent diverse backup. However, manual operator actions can serve as an acceptable diverse backup but only if a suitable human factors engineering analysis is performed to demonstrate that BTP 7-19 acceptance criteria for plant conditions are satisfied. It is noted that actions with limited temporal margin (e.g., less than 30 minutes) will receive detailed staff review.

DI&C-ISG-02 also addressed the effects of CCF; specifically, it clarified whether spurious activations should be considered in CCF evaluations. The ISG states that potential spurious trips and actuations are self-announcing so they are generally of a lesser safety concern than failures to trip or actuate. The ISG concludes that "the effects of failure to actuate and the effects of spurious trips and actuations should be evaluated to ensure the effects are bounded by the plant design basis."

BTP 7-19 was revised to incorporate the guidance and acceptance criteria established in DI&C-ISG-02. Rev. 6 of BTP 7-19 was issued in March 2010. In addition, it provides additional clarification on the four-point position by including a definition of "best-estimate" analysis and introducing guidance on the independence of diverse means of actuation. It also addresses manual actions as a diverse means of actuation, the relationship between CCFs and diverse means of actuation, diversity considerations for automated and manual actions, the diversity and CCF considerations when combining RTS and ESF actuation systems in a single controller or central processing unit, treatment of failure to actuate and spurious actuation, and identification of design attributes that eliminate consideration of CCF. Additionally, the specification of acceptance criteria was expanded to correspond to the guidance incorporated from DI&C-ISG-02.

NUREG/CR-6303 provides guidance on performing a diversity and defense-in-depth (D3) assessment to determine the CCF vulnerability of an NPP I&C system architecture. This guide is an expansion of NUREG-0493. NUREG/CR-6303 analysis begins by decomposing of the NPP I&C system architecture into a block representation, followed by determination of which blocks are susceptible to a postulated CCF. The assessment of CCF vulnerability involves identification of common elements, interdependencies (e.g., physical, logical), and diversities. Following this determination, assessment of defense-in-depth can proceed.

As established in NUREG/CR-6303, assessment of defense-in-depth is performed by postulating concurrent failures of identical (or nondiverse) blocks in all redundant divisions or lines of defense while performing "best-estimate" safety analyses of Chapter 15 events from the plant safety analysis report (SAR). If the estimated plant response exceeds specified limits for any AOO or DBA in the presence of postulated CCF, then a CCF vulnerability exists and corrective action, such as the introduction of additional diversity, should be taken to ensure adequate protection is provided, unless the choice of no corrective action can be otherwise justified.

When additional diversity is needed to mitigate an identified CCF vulnerability of one or more safety functions, that diversity can be achieved through provision of a separate automatic system to back up the disabled safety function(s) or through the introduction of intentional diversity and compensating design measures at the appropriate lower level(s) of the I&C system architecture (e.g., system, divisional redundancies, subsystems, modules, or components). If a potential vulnerability is determined, a more detailed evaluation of the CCF susceptibilities and corresponding mitigation approaches can benefit from a block representation with finer granularity than the high-level black box approach.

The guidance in NUREG/CR-6303 provides a set of six diversity attributes with several diversity criteria within each attribute. However, because of the number of criteria in each attribute coupled with the number of attributes, the number and complexity of possible combinations of attributes that could be used to achieve adequate diversity in a safety system make the guidance very difficult to use as a safety assessment tool. Consequently, a subjective judgment is required to determine what diversity usage is adequate to mitigate identified CCF vulnerabilities.

As part of recent regulatory research, the basis for establishing diversity strategies was developed. NUREG/CR-7007, “Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems [14],” describes the technical basis for establishing acceptable mitigating strategies that resolve D3 assessment findings and conform to U.S. NRC requirements. This NUREG also presents a comparison tool for assessing the relative impact of different diversity choices.

As documented in NUREG/CR-7007, the approach for establishing diversity strategies involved capturing expert knowledge and lessons learned, determining best practices, and assessing the nature of CCFs and compensating diversity attributes. The basis for the identified strategies centers on practices derived from examples of diversity usage by the international nuclear power industry and several nonnuclear industries with high-integrity and/or safety-significant I&C applications.

3 CONTEXT FOR REEVALUATING NRC POSITION ON CCF

In its current position, NRC staff considers that software design errors and software programming errors are credible sources of CCF for digital safety systems. In the SRM to SECY 93-087 the Commission concluded that vulnerabilities to CCF should be assessed. 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 are established in regulation and associated regulatory guidance. Criteria for assessing adequate diversity are provided within the review guidance given in SRP BTP 7-19. However, diversity is not a substitute for, nor should it be proposed instead of the independence required by regulation and by standard (50.55a). Rather, diversity should be seen as a necessary accessory to independence for increasing system robustness in the face of unidentified common-mode failures.

The current policy and guidance considers necessary a diversity and defense-in-depth analysis to address CCF vulnerabilities. This is presently the case for computer-based safety systems and would be the case for new-technology safety systems whose reliability properties are imperfectly known. The diversity and defense-in-depth assessment method documented in NUREG/CR-6303 is considered as acceptable for addressing vulnerabilities to common-cause failures in protection systems. Although there are a number of cases where NPP systems can cope with the CCF of digital systems or provide mitigation using other systems or manual actions, the accepted method to address CCF in the absence of such conditions is through application of diversity.

In addition, industry stakeholders have asked NRC staff to consider defensive measures to eliminate CCF from further consideration. Guidance in BTP 7-19 includes two design attributes, which, if satisfied, can be used to eliminate from further consideration the potential for software CCF. These attributes are based on a demonstration that adequate internal diversity exists, or assurance that the systems are sufficiently simple that all possible software failure paths can be tested for and shown to be non-existent. The staff recognizes the need for further development and refinement of regulatory guidance on diversity attributes and the use of risk evaluations of digital systems.

Based on this, NRC staff is developing the technical basis associated with potential for CCF in digital systems. In addition the NRC staff is developing proposed guidance for low risk-significant systems without modifying the current NRC position on CCF and evaluating longer term recommendations, which are described in the integrated action plan. This effort may include changes to certain regulatory guidance that, while maintaining the current NRC position on CCF, provide additional guidance that could result in more digital systems being implemented in the near term. This would be the first part of the review, while the complete reevaluation of the NRC position on CCF is moving forward at a lower priority.

4 CHALLENGES POSED BY DIGITAL TECHNOLOGY

The evolution of I&C systems in NPP applications has undergone three generational changes. The first generation saw the use of analog technology for instrumentation and mechanical relay based technology for control of discrete processes. The second evolutionary generation saw the use of discrete or integrated solid-state equipment for both instrumentation and control. The third evolutionary change saw the replacement of the functions of mechanical relays by the programmable logic controller (PLC). The PLC itself became possible by the advent of the microprocessor in the 1970s. Initially, PLCs were used in non-nuclear applications, but their (evolving) capabilities in handling large amounts of input/output (I/O) devices, large volumes of data, mathematical computations and continuous process control functions contributed to their introduction to the non-safety applications in nuclear power plants. By the early 1990s, microprocessors were being used for data logging, control, and display for many non-safety related functions. Currently, digital I&C systems have been used in many applications in NPPs, including feedwater control systems, recirculation control systems, demineralizer control systems, reactor protection system, and main turbine controls. In addition, digital I&C systems have been employed in a limited number of safety systems within the United States.

In the 1990s, digital safety systems based on the Westinghouse Eagle 21 platform and the Foxboro Spec 200 Micro platform were licensed and implemented in a few U.S. NPPs. By the early 2000s, the NRC issued the first of several generic, non-site-specific approvals of specific digital I&C control system platforms for use in safety applications. The current trend for the evolution of digital I&C systems in NPPs is to develop digital safety-related I&C platforms based on field-programmable gate array (FPGA) technology. Some of the major drivers towards the continued development and use of digital technology in NPPs include technology obsolescence of existing systems and the widespread use of digital technology in non-nuclear industries.

The development and utilization of digital I&C systems in NPPs, as well as utilization in non-NPP industries, have demonstrated several major strengths and weaknesses of digital I&C systems. Several of these strengths and weaknesses, as well as unique characteristics, of digital technology are discussed below.

- **Digital systems have potential for high reliability** – Reliability implies the probability that a system will be able to identify and/or remove a fault before it prevents a system from performing its function. The most common fault-identification and removal technique is testing. Software introduces a powerful means of providing online embedded diagnostics and self-checking capability.
- **Digital systems have high flexibility** – Flexibility is a key attribute of digital systems. That is, they can be designed to be easily configurable and portable. Another aspect of flexibility is "reusability." The same microprocessor-based system can be easily reloaded with different software to perform a completely different set of functions.
- **Digital systems typically have combined functionality** – A digital system may be designed to perform multiple functions (e.g., acquire input data, process the data, perform onboard diagnostics, monitor alarmed conditions, etc.). This characteristic has the potential to negatively affect important plant or I&C functions such as the quality of closed loop control and reaction times of the human-system interactions.
- **Failure modes are less well understood** – Analog circuitry generally has fixed and testable functionality. The error modes of analog circuitry (hysteresis, sticking, wear, corrosion, drift, etc.) are well understood and while the potential for common mode effects also exist, these are typically well controlled and fully testable. By contrast, software cannot be fully tested and is typically highly nonlinear, implying tests cannot be extrapolated to cover regions that are not completely tested. Also, software does not age in the traditional sense (i.e., wear out) and therefore errors cannot be identified by periodic maintenance as in analog systems.

- **The presence of software introduces greater potential for systematic faults in the design, implementation, operation, and maintenance/configuration management** – Implementation of system functions in software does introduce greater potential for systematic faults in the design, implementation, operation, and maintenance/configuration management. This also increases the probability of the introduction of common-mode software failures that can cause redundant safety systems to fail in such a way that there is a loss of safety function. While techniques exist for evaluating common-mode failure potential in analog devices, current techniques for evaluating software common cause failures are much less mature. The method available for evaluating software diversity as a means of assuring independent redundant channels for a nuclear application suffer from a lack of supporting data, and effective benchmarking to prove their effectiveness.

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. While diversity and other design measures have been traditionally coupled with high-quality practices for conventional safety systems to mitigate the potential for common design errors or defects in common components, the complexity of digital I&C components and the less predictable nature of software behavior lead to greater uncertainty in demonstrating that undetected systematic faults are avoided in the design, implementation, and operation of digital safety systems. Specifically, although a great deal of effort has been applied to develop highly reliable software with extremely low failure rates, current software engineering practice has not achieved the capability to demonstate quality and reliability through testing and analysis under all credible conditions.

A high quality development and implementation program is necessary to detect and correct digital I&C development and implementation errors (i.e., faults). However, as design complexity increases, the feasibility of exhaustive testing or comprehensive formal proof diminishes considerably. Therefore, some residual faults may remain undetected and persist as latent faults within the system. Design errors arising from flawed, incomplete, ambiguous, or misinterpreted requirements are systematic in nature and resulting faults are significantly more difficult to detect and correct as the system life-cycle phases progress.

Analyses of analog system design using methods based on first principles and tests using these methods to establish a reasonable expectation of continuous performance over substantial ranges of input conditions are important and proven capabilities. These analysis and test capabilities enable extensive use of type testing, acceptance testing, and inspection of design outputs in assessing the design of analog systems and components. If the design process assures continuous behavior over a fixed range of inputs, and testing of a finite sample of input conditions in each of the continuous ranges demonstrates acceptable performance, then performance at intermediate input values between the sample test points can be logically inferred to be acceptable with a high degree of confidence. It is this aspect of analog systems, not their "simplicity," that distinguishes them from digital systems. In fact, analog systems are not always more simple than digital systems. Digital I&C systems are fundamentally different from analog I&C systems, in that minor errors in design and implementation can cause digital systems to exhibit unexpected behavior. Consequently, the performance of digital systems over the entire range of input conditions cannot generally be inferred from testing a sample of input conditions. Inspections, type testing, and acceptance testing of digital systems and components do not alone establish a sufficiently high level of confidence that the design is predictably safe. To address this issue, inspection and testing are used to verify correct implementation and to validate desired functionality of the final product, but confidence that isolated, discontinuous point failures will not occur derives from and is dependent on the discipline of the development process. This consideration is true whether the digital systems are relatively simple or very complex.

In digital I&C safety systems, requirements, specifications, code, data transmission, data, and hardware may be common to redundant divisions and/or functions. Although this commonality is the basis for many of the advantages of digital systems, it also raises a key concern: a design using shared data or code has the potential for a common-cause failure, defeating the redundancy achieved by the hardware architecture. The issue of common-cause failure in digital systems has been widely known in the digital system research community for more than thirty years. Several well-known studies [15, 16] have demonstrated that separate digital systems developed to satisfy the same function requirements can fail in a statistically dependent way. One of the key issues is that there are very few, if any methods, for providing equivalent reasonable assurance of safety because of challenges associated with adequate modeling. One method that has been proposed is to limit systems in terms of simplicity to only those that are so "simple" that they should be treated as analog systems for the purpose of consideration of software/logic based common cause failures. This reasoning suggested that some digital systems are sufficiently "simple" that a testing approach that can eliminated the potential for an unanalyzed failure to occur would be an acceptable approach. However, there are multiple interpretations of what is necessary for to effectively test out all potential failure modes (i.e. 100% testing). One interpretation suggests testing all possible combinations of input and output values is sufficient. But if the device is not stateless (i.e., if it retains some internal memory of the past), then the internal state registers and their possible values need to be treated like, and in combination with, the inputs in the determination of the test cases. This is also true of external conditions (i.e. initial or boundary conditions on the device). This approach logically then requires that all possible states of the device have to be knowable and known, so that test metrics can be developed and demonstrated to be complete. This then leads to a definition of a "simple" that would include some method of demonstration that all states have been tested.

There are some experts who argue that logical separation should be taken into consideration in order to reduce the number of required test cases. For example, if the FPGA design implements two functions that cannot electrically or logically interfere with one another, then one might argue they can be tested separately and thus reduce the number of tests needed. An equivalence class argument (similar to what is done in fault injection testing) could also be put forth to reduce the testing requirement. Regardless of the methods used, there needs to be some combination of analysis and test that would demonstrate to a sufficient level of confidence that software CCF are not possible. The threshold is high not because of the low probability or low consequence of potential common cause failure, but because we are sufficiently confident that we can eliminate consideration of them completely for a particular device. Essentially, the argument is that the analysis and testing of these systems (simple systems) will provide as much confidence as an analysis of analog systems, because we can use testing and analysis to know the systems will perform as designed and not experience software common cause issues.

The significant challenges associated with evaluating CCF design and analysis standards for digital systems include: 1) the difficulty in modeling digital system failure modes, 2) the difficulty of assessing the likelihood of digital system (particularly software) failures, 3) the difficulty in assessing what can go wrong when digital systems fail, and 4) the challenges with development and using digital (particularly software) failure data in the analysis of digital system failures. Current review guidance in BTP 7-19 includes two criteria, which, if satisfied, can be used to eliminate from further consideration the potential for software CCF, based on a demonstration that adequate internal diversity exists, or based on assurance that the systems are sufficiently simple that all possible software failure paths can be tested for and shown to be non-existent. The staff's position was last enunciated to the Commission in SECY 09-0061, "Status of the Nuclear Regulatory Commission Staff Efforts to Improve the Predictability and Effectiveness of Digital Instrumentation and Control Review" [17].

To resolve the challenges discussed above it would be helpful to be able to determine how improved requirements and guidance on the use of digital system design processes have improved digital systems and reduced their failure rates. However, despite the best efforts of designers, developers, implementers, reviewers, testers, suppliers, and assessors, errors happen. In particular, the types of failures that can compromise safety-critical functions typically arise from design mistakes or implementation errors. Failures can also result from undetected internal flaws (i.e., platform faults), system interactions, and external effects. Hazard identification and design measures can minimize the potential for some sources of failure, but unanticipated and untested conditions can still pose a risk. Some well-known digital system errors include the Therac 25 Overdoses in the late 1980s, the Patriot Missile Battery intercept failure in 1991 and the destruction of the Ariane 5 missile in 1996.

Some researchers in the field have argued that the effective use of more effective digital system design processes and defensive design measures have significantly reduced the likelihood of digital system failures, however, significant digital system errors continue to lead to significant failures. Some significant recent software failures include:

- Over the past two years Nissan has been recalling airbags for over 1 million cars due to a software glitch that the affected cars could not detect whether an adult was in the passenger seat and as a result the airbags would not inflate. There has been a reported two accidents due to this software failure.
- In February 2014 Toyota recalled almost 2 million Prius in order to fix a software error with its engine control unit. This software glitch could lead to transistors overheating, sending the car into fail-safe mode and potentially causing the hybrid system to shutdown while driving. The same software problem caused Toyota to recall another 625,000 vehicles in July 2015.
- In March 2015 F-35 aircrafts experienced a serious software failure preventing the aircraft from detecting targets. The sensors on the plane could not tell the difference between singular or multiple threats.

Therefore, the staff is working with industry stakeholders to identify possible design attributes that can be used to reduce the likelihood of digital system failures

To identify insights related to improving D3 evaluations and methods for protecting plants against digital I&C related CCFs that could disable safety functions and thereby degrade plant safety, several groups have reviewed the operating experience of U.S. NPPs. These have included studies of specific systems and general industry trends based primarily on operational experience databases. These studies include [18, 19, 20] analysis of the general classes of failures (Jackson and Brill and EPRI for example) and studies of specific systems (Bickel) based on data that is available. In the first two studies, the accident sequence precursor and licensee event report databases were examined and evaluated to determine the kind of failures reported for digital system and their causes. The events were characterized in terms of their causes, effects, and associated corrective actions. In the vast majority of the reported failures there was no potential for CCF and only one failure was caused by a software design error, however there were a number of potential CCFs identified. Although these studies indicated that digital system CCF are unlikely, the significant limitations associated with the studies mitigate the values of these findings. Neither attempted to estimate the population of the components in use nor how representative the failures studied were of the actual population of systems in use. Also the level of detail available in the data used in the studies is very low, and coding rules are not well defined. This may lead to the same failures categorized differently in each study, indicating possible challenges of reproducibility. The largest challenge with this kind of analysis is that it simply can not (because of the level of detail of the information available in the databases) evaluate the likelihood of potential software errors in unanalyzed digital systems. In the Bickel study, the analysis was conducted to evaluate failure rates of a particular system in greater detail. In this study the CE core protection calculator system was examined. Although there was significant operational data to make a reasonable assessment of the failure rates and common cause failure rates of this systems, the lack of significant details on how the software errors were generated make it hard to generalize these results.

An additional challenge in characterizing digital system failures, particularly in the nuclear power plant arena, is that extensively detailed studies of actual and potential systems failures of systems used in safety systems are limited. In November 1994, it was discovered that although a safety related sequencer in a nuclear power plant was supposed to allow valid safety injection (SI) signal to pass thru while in test mode, a logic defect inhibited valid SI signal during testing. The root cause was determined to be inadequate software design, coupled with inadequate software verification and validation (V&V). This digital system was deployed with a selectable automatic self-test feature. It was discovered later, during surveillance testing, that 5 of 18 automatic self-test routines running in each of asynchronous sequencer channels had an error in the application logic that would have prevented an actual SI signal from passing through while in auto test mode. It is interesting to note that adding automated self-testing features to the relatively simple safety function logic led directly to the problem. Further analysis and tests demonstrated that operators would have recognized the condition during a loss of coolant accident (LOCA) and manually initiated safety injection in time to stay within acceptance criteria.

Some relatively recent studies [21, 22, 23] have analyzed safety systems and risk significant non-safety systems used in operating nuclear power plants. The first study, of a component of a protection system shows that even after 9 years of service, in addition to the development and pre-installation testing, 14 faults were found residing in the software via inspections and fault injections. It is statistically believed more faults reside in the software. This finding was based upon the assumption that the software requirements were correct, which is a significant assumption as NASA internal data shows about 40% of software failures were caused by requirements errors. Five of these 14 faults are characterized as missing functions which were specified in the software requirement, three as incomplete and inadequate implementations. The majority of these faults may lead to inadequate system healthy self-monitoring. The rest of the 6 faults are missing validations for the input or internal state variables. In the second study it was found that detailed simulation of the digital system and all system inputs and well as the timing and sequencing of these inputs were needed to adequately capture the unique failure modes associated with the system. The study also found that the lack of effective methods for comparing digital system failure modes and likelihoods and accounting for uncertainty, particularly epistemic uncertainty, severely limits the capability analysis techniques to predict the effects of digital systems on plant safety.

The international community has looked at the benefits of using digital systems, and establish ways to ensure software CCF does not undermine benefits presumably gained. Current international approaches consider all CCFs and select multiple CCFs (any that dominate a plant's risk profile) as postulated initiating events that should be considered in the design basis and addressed through conservative analysis. This may be seen as differing from NRC policy implementations to date, which focus on a single CCF of a single protection system, treat the failure as beyond design basis, and allow use of best estimate analysis when assessing their impact on safety.

Over time, the perspectives have formulated, enhanced, and reinforced fundamental safety concepts and safe design principles. In doing so, the international approach to adequately address CCF continues to rely upon fundamental design principles of independence, defense-in-depth, and diversity. For example, Multinational Design Evaluation Programme (MDEP) Digital I&C Working Group (DICWG) established Generic Common Position DICWG No. 1 [24] on the treatment of CCF caused by software within digital safety systems. It acknowledges CCFs as a significant safety concern when software has some common dependency. It also acknowledges the need for protection from the effects of CCFs due to software in DI&C safety systems. This common position identifies four positions for the treatment of software CCF.

Current international guidance relies on deterministic analysis and acceptance criteria, because it recognizes challenges associated with effectively and efficiently applying probabilistic risk analyses with clearly understandable acceptance criteria for complex digital systems. International organizations also recognize that technical basis to acceptably apply such an approach has not been developed or validated.

More recent international guidance discusses the concept of defensive measures. For example, IAEA NP-T-1.5 [25] recognizes implementation choices, constraints and testing lessen the likelihood of CCF. It also acknowledges the possibility of implementing defensive measures (i.e., design features and characteristics that preclude, avoid or limit the propagation of some types of CCFs). Regardless, it directs an evaluation of the impact of such malfunctions and the implementation of mitigating features, where needed, to maintain an acceptable level of safety. Nonetheless, these discussions, which would promote application of defensive measures and engineering judgement as justification of reasonable assurance that CCF likelihood is low enough to exclude a component from further CCF consideration, are inconsistent with current NRC policy. International guidance expects a demonstration of the effectiveness of any defensive measures that are included in a design.

NRC staff is also evaluating non-nuclear power generation industries. However, challenges exist when evaluating this approach because non-nuclear industries treat safety assurance differently than NPPs, and these differences may cause comparisons between industries to be misleading. Most non-nuclear guidance generally does not explicitly require diversity or defense-in-depth attributes or explicitly segregate software CCF from the other forms of failure or maloperation, which should be addressed in hazard analysis. Nevertheless, some non-nuclear guidance includes the principles of separation and independence, including measures to prevent failure propagation, which are consistent with the nuclear principle of defense-in-depth. The chemical process industry includes the concept of diversity between the basic process control system and the safety instrumented system, which represent two layers of a defensive architecture. Applicable chemical process guidelines state the design of a safety system must address diversity. Additionally, NRC staff guidance for fuel-cycle facilities includes the principles of diversity and defense-in-depth in its treatment of items relied on for safety.

The National Research Council published a 1997 National Academies report on "Safety and Reliability Issues associated with Digital Instrumentation and Control Systems in Nuclear Power Plants" [5] that includes a discussion of software CCF, safety and reliability assessment methods, the related U.S. nuclear regulatory approach, and approaches used in non-nuclear industries. The report notes that regulatory agencies outside of nuclear power do not, in general, have equivalent policies about common-mode software failure. One of the conclusions reached by the committee that wrote the report was: "The USNRC should retain its position of assuming that common-mode software failure is credible."

These non-nuclear industries apply different approaches to safety assurance than the nuclear industry. Furthermore, unlike the nuclear industry, non-nuclear industries do not create an explicit distinction of safety and non-safety systems. Additionally, non-nuclear industries generally apply a graded-approach to software development based upon the software's potential to contribute to hazards, as identified through a systematic hazard analysis.

5 IMPLICATIONS

As part of this effort to reevaluate the current position on CCF, it is noted that it does not include specific criteria to characterize the likelihood of software CCF and eliminate it from further consideration in a D3 analysis. The review of the evaluation of digital system technology and analysis methods discussed in this paper has begun the process of assessing the underlying technical basis associated with CCF and provide the technical support for updating the NRC position on potential CCF in digital systems while enhancing efficiency, clarity, and confidence. The use of risk information might be able to provide additional information on the most appropriate methods to grade the needed level of assessment of the consequence of digital CCF, but it has been challenging to develop specific criteria based on risk analysis. A number of studies have been done to look at the likelihood of software failures as well as the consequences to plant safety. Some papers [20, 21, 22, 23] have described efforts that have been successful in providing some insight at the likelihood of failure of digital systems used in nuclear power plants. Although reliability of software based digital systems has become a fairly mature field, translating that information into effective risk analysis is still evolving. Quantitative assessment of software reliability is not easy and frequently depends on data that does not exist or is hard to generalize; estimating the fraction of failures that could lead to CCFs is even harder. While there is guidance on ways to develop risk analysis for digital systems, including CCF, available in a number of national and international standards [26, 27], the larger concern is how much confidence can be provided by these analyses given the high uncertainty in not only the reliability analysis but also the underlying hazard analysis.

As discussed above one of the challenges with analysis of digital systems are the nonlinear effects and the fact that digital system failures (particularly software) are not bound by physical laws. This makes the first part of the risk triplet (what can go wrong) particularly difficult and places a heavy burden on the digital system hazard analysis.

Qualitative assessment of the likelihood of various CCF causes may be possible, but at least at this point, must not be used without care. There are several possible ways to manage the risk of digital CCF. These include eliminating the risk, mitigating the risk, or accepting the risk. In the current NRC position on digital CCF, eliminating the risk, amounts to a demonstration that under certain design constraints CCF is not a concern (such as, internal diversity or diverse means to accomplish the design function). To accept the risk, under the current position one would conduct a D3 analysis and demonstrate that the consequence of the CCF does not exceed the acceptance criteria. Both these options should continue to be part of the NRC position. The third option is to mitigate the risk, this is where use of both risk informed grading and more effective guidance on methods to cope with digital CCF could be effective. In IAEA NP-T-1.5 [25] similar choices are outlined. The NRC may also be able to use information discussed above from non-nuclear industries to help build a structure to effectively apply a graded-approach based upon the software's potential to contribute to hazards. The NRC staff will continue to evaluate the information discussed above as it develops recommendations on how to reevaluate the current position on digital CCF.

6 CONCLUSIONS

This paper has discussed some of the challenges faced with setting a technical policy associated with what is needed to assure adequate requirements for digital system common mode failure. Although the authors have found that significant progress has been made in improving digital system design and implementation, digital system failures continue to occur. Because of the limitations associated with the state-of-the-art in digital I&C system analysis, it will be difficult to recommend a modification of the current consequence bases regulatory position currently used by the NRC. However, there is evidence that improved design processes and methods have most likely reduced the likelihood of digital system failures and CCFs, so improvements in terms of risk informed grading of the CCF requirements may be appropriate. Although most of the work to scope the issues, evaluate digital system experience and assess the current state-of-the-art of digital system assessment methods has been done, additional effort is needed to determine the most appropriate methods for assuring safety and determining, if the NRC staff should recommend reaffirming or revising the current NRC position on CCF in digital systems.

7 REFERENCES

1. SRM to SECY 15-0106, *Proposed Rule: Incorporation by Reference of Institute of Electrical and Electronics Engineers Standard 603-2009, "Criterial for Safety Systems for Nuclear Power Generating Stations*, U.S. Nuclear Regulatory Commission, Washington, D.C., 2016

2. U.S. Nuclear Regulatory Commission, "Guidance for Evaluation of Diversity and Defense in Depth in Digital Computer Based Instrumentation and Control Systems", NUREG-800, BTP-7-19, August 2019.

3. NUREG-0493, *A Defense-in-Depth and Diversity Assessment of the RESAR-414 Integrated Protection System,* NRC, Washington D.C., March 1979.

4. 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., 2016.

5. National Research Council, *Digital Instrumentation and Control Systems in Nuclear Power Plants: Safety and Reliability Issues*, National Academy Press, ISBN: 0-309-52444-X, Washington, DC, 1997.

6. SECY 91-292, “Digital Computer Systems for Advanced Light-Water Reactors” U.S. Nuclear Regulatory Commission, Washington, D.C., 2016.

7. 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., 2016.

8. *EPRI Advanced Light Water Reactor Utility Requirements Document*, Revision 4, Electric Power Research Institute, 1992.

9. IEEE Std 603-1991, *Criteria for Safety Systems for Nuclear Power Generating Stations*, Institute of Electrical and Electronics Engineers, Inc. Piscataway, NJ, 1991.

10. IEEE Std. 7-4.3.2-2003, “Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations,” Institute of Electrical and Electronics Engineers, Piscataway, NJ, 2003.

11. U.S. Nuclear Regulatory Commission, Regulatory Guide 1.152 Criteria for Use of Computers in Safety Systems of Nuclear Power Plants.” Revision 3, NRC, Washington, D.C., June 2011.

12. G.G. Preckshot, *Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems*, NUREG/CR-6303, NRC, Washington, D.C., December 1994.

13. U.S. Nuclear Regulatory Commission, “Digital Instrumentation and Controls, DI&C ISG-02, Task Working Group #2: Diversity and Defense-in-Depth Issues,” Revision 2, NRC, Washington, DC, June, 2009.

14. R.T. Wood, R Belles, M.S. Cetiner, et. al, *Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems*, NUREG/CR-7007, NRC, December 2008.

15. B. Littlewood, “The Impact of Diversity Upon Common Mode Failures”, *Reliability Engineering and System Safety*, **Vol 51, Issue 1**, pp 101-113, 1996.

16. J. C. Knight and N.G. Leveson, “ An Experimental Evaluation of the Assumption of Independence in Multiversion Programing”, IEEE Transaction on Software Engineering, Vol 12, Issue 1, pp 96-109 1986.

17. SECY 09-0061, “Status of the Nuclear Regulatory Commission Staff Efforts to Improve the Predictability and Effectiveness of Digital Instrumentation and Control Reviews”, U.S. Nuclear Regulatory Commission, Washington, D.C., 2016.

18. T.W. Jackson and R.W. Brill, “A Study of Nuclear Power Plant Events that Involve Instrumentation and Control Systems”, *Proceeding of the International conference on Nuclear Energy* (ICONE 8), Baltimore, MD, April 2000.

19. EPRI 1016731, *Operating Experience Insights on Common Cause Failures in Digital Instrumentation and Control Systems*, EPRI, Palo Alto, CA, December 2008.

20. J. Bickel, “Risk Implication of Digital Reactor Protection System Operating Experience,” *Reliability Engineering and System Safety*, **Vol 93, Issue 1**, pp 107-127 2008.

21. Y Shi, M. Li, S.A. Arndt and C. Smidts, “Metric-based Software Reliability Prediction Approach and its Application,” *Empirical Software Engineering*, **Vol 21, Issue 3**, pp 1-55, June 2016.

22. S.A. Arndt, and A. Kurizky, "Lessons Learned from the Nuclear Regulatory Commission's Digital System Risk Research," *Nuclear Technology*, **Vol 173, No. 1**, pp 2-7, January 2011.

23. T. Aldemir, S. Guarro, D. Mandelli, J. Kirshenbaum, L. A. Mangan, P. Bucci, M. Yau, E. Ekici, D.W. Miller, X. Sun, and S.A. Arndt, "Probabilistic Risk Assessment Modeling of Digital Instrumentation and Control Systems Using Two Dynamic Methodologies," *Reliability Engineering and System Safety*, **Vol 95**, pp 1011-1039, October 2010.

24. Multinational Design Evaluation Programme (MDEP) Digital I&C Working Group (DICWG) Generic Common Position DICWG No. 1, "Common Position on the Treatment of Common Cause Failure Caused by Software within Digital Safety Systems, June 2013.

25. IAEA Nuclear Energy Series No. NP-T-1.5, *Protecting Against Common Cause Failures in Digital I&C Systems of Nuclear Power Plants*, International Atomic Energy Agency, Vienna, 2009.

26. U.S. Nuclear Regulatory Commission, *Probabilistic Risk Assessment and Severe Accident Evaluation for New Reactors,* NUREG – 0800, Chapter 19.0 Rev 3, NRC, Washington, D.C., December 2015

27. International Electrotechnical Commission, "Functional safety of electrical/electronic/ programmable electronic safety-related systems – Part 6: Guidelines on the Application of IEC 61508-2 and IEC 61508-3," IEC 61508-6, Geneva, Switzerland, 2010.