ADDRESSING EMBEDDED DIGITAL DEVICES IN SAFETY-RELATED SYSTEMS OF NUCLEAR POWER PLANTS

Richard Wood
The University of Tennessee
Knoxville, TN 37996-2300
woodrt@utk.edu

Jerry Mauck
JLM Engineering and Technology Resources
5234 Green Bridge Road
Dayton, Maryland 21036
jerrymauck@verizon.net

Edward Quinn
ANS Past President
Technology Resources
23292 Pompeii Drive
Dana Point, CA 92629
tedquinn@cox.net

ABSTRACT

The purpose of this paper is to provide an overview of the development of the approach to addressing embedded digital devices (EDD) in safety-related systems of nuclear power plants in the U.S. and around the world. In April, 2016, the U.S. Nuclear Regulatory Commission (USNRC) issued RIS 2016-05 to heighten awareness that EDDs might exist in procured equipment used in safety-related systems without the devices having been explicitly identified in procurement documentation. Inadequate consideration of these devices in digital technology system upgrades, component replacements, and new equipment applications could lead to an adverse safety consequence. The USNRC request was for addressees to implement early efforts to identify these devices. An area where this is being addressed is in regard to the performance of Diversity and Defense-In-Depth (D3) analyses, as addressed in USNRC Branch Technical Position 7-19.

Nuclear facilities have increased their use and reliance on digital technology in systems and equipment (e.g., I&C, electrical systems, and fluid systems). In addition to digital instrumentation and control (I&C) systems, examples of safety-related equipment that may use digital technology include emergency diesel generators, pumps, valve actuators, motor control centers, breakers, priority logic modules, time-delay relays, and uninterruptible power sources.

In the U.S. and around the world, engineering and licensing activities in standards and guidance have been, and are being developed to address this important consideration in protecting safety-related systems. This paper addresses development of an extended approach to evaluating common-cause failure vulnerability and mitigation in regard to equipment with an EDD.

Key Words: embedded digital device, common-cause failure, diversity, defense-in-depth

1 INTRODUCTION

The reliability, high-functionality and flexibility characteristics of digital technology have led to widespread adoption of digital instrumentation and control (I&C) systems and digitally-augmented equipment by most process industries. Since these industries dominate the instrumentation marketplace, the availability of non-digital equipment has diminished considerably. In addition to adapting to constraints arising from marketplace availability, the nuclear industry has incentive to transition to increased use of digital technology. This transition can result in benefits such as resolution of obsolescence pressures, improved efficiency through enhanced functionality, increased accuracy, speed, and quantity of transmitted data, and improved reliability with robust fault detection.

Although the aforementioned benefits may be achieved through increased use of digital technologies, there is concern about the potential for common-cause failure (CCF) vulnerabilities resulting from shared software (or software-designed) features among equipment with embedded digital devices (EDDs). The U.S. Nuclear Regulatory Commission (USNRC) recently issued a Regulatory Issue Summary (RIS) [1] on potential safety issues associated with the use of equipment with EDDs in safety applications. The RIS expresses the staff concern that "increased use of EDDs in safety-related equipment may increase a facility's vulnerability to a CCF, or otherwise degrade equipment reliability that could adversely affect safety" and serves to heighten awareness of the issue.

The USNRC RIS defines an EDD as "a component consisting of one or more electronic parts that requires the use of software, software-developed firmware, or software-developed programmable logic, and that is integrated into equipment to implement one or more system safety functions." It further notes that firmware includes "programmable logic devices, field programmable gate arrays, application specific integrated circuits, erasable programmable read only memory, electrically erasable programmable read only memory, and complex programmable logic devices." Equipment with EDDs can include sensors, breakers, priority logic modules, time-delay relays, pumps, valve actuators, motor control centers, and uninterruptible power supplies.

2 REGULATORY BASIS RELEVANT TO TREATING EQUIPMENT THAT CONTAINS AN EDD

The aforementioned RIS clarifies the USNRC position on regulatory requirements for quality and reliability as applied to safety-related equipment containing EDDs. However, it does not require any specific action or response. Instead, the RIS discusses the issues associated with EDDs and identifies prevailing regulatory positions and guidance. In particular, Branch Technical Position (BTP) 7-19, "Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems," [2] of the USNRC Standard Review Plan Chapter 7 [3] is cited in regard to assessing and mitigating the impact of CCF.

The USNRC policy regarding treatment of digital CCF is provided in the Staff Requirements Memorandum (SRM) on SECY 93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs" [4]. Item II.Q of SECY 93-087 [5] notes that hardware design errors, software design errors, and software programming errors are credible sources of CCF for digital safety systems and establishes a four-point defense-in-depth and diversity position. The SRM identified digital CCF as a beyond design basis event; thus, the four-point position was modified to specify best-estimate analyses of the impact of CCF and to allow non-safety systems to perform diverse functions.

As noted, BTP 7-19 provides guidance for the evaluation of compliance with the four-point position established in the SRM to SECY 93-087. The D3 assessment method documented in NUREG/CR-6303, *Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems* [6], is cited in BTP 7-19 as acceptable for demonstrating that vulnerabilities to CCFs have been adequately addressed.

The guidance in the BTP generally focuses on system-level consideration of CCF and does not explicitly address treatment of equipment with an EDD. However, it does identify design attributes such as simplicity that can eliminate further consideration of CCF within a D3 analysis. Specifically, internal diversity and testability are two design attributes that are sufficient to eliminate CCF concerns. The BTP specifies a case-by-case treatment for the evaluation of whether sufficient diversity is provided based on the attributes defined in NUREG/CR-6303. Regarding testability, the BTP specifies that "every possible combination of inputs, internal and external initial states, and every signal path" should be testable and should demonstrate acceptable performance.

Other than the RIS, the authors did not find many relevant regulatory positions or evaluations focused on component level CCF considerations. The signal diversity attribute suggests the use of diverse sensors but it includes a criterion allowing for redundant sets of sensors measuring the same parameter for different systems, which can only be characterized as an extremely limited form of diversity. The criteria for the equipment diversity attribute within NUREG/CR-6303 touch on component level diversity in terms of the microprocessor itself (different processor architectures and different chip versions). However, the application of diversity is not explicitly extended to other digital components (e.g., analog-to-digital convertors, media access chips). Although no specific examples of regulatory evaluations were found addressing particular board-level digital components beyond microprocessors, it is recognized that such considerations may have been embedded in conclusions on system-level diversity and that the technical details giving clear indication of those considerations may have been withheld to protect proprietary information.

Finally, the guidance on command prioritization in Digital I&C Interim Staff Guidance 04 (DI&C-ISG-04), "Task Working Group #4: Highly-Integrated Control Rooms—Communications Issues (HICRc) Interim Staff Guidance" [7], specifies that priority module designs should be fully tested to minimize the probability of failures due to common software. This corresponds to the 100% testability design attribute of BTP 7-19 and is applicable to digital priority logic components.

3 PROCESS FOR ADDRESSING CCF IMPACT OF AN EDD

3.1 Consideration of EDDs for Existing or New Reactors

Regarding consideration of the potential impact of equipment with an EDD within the I&C architecture of existing or new reactors, a primary concern is shared software or software-designed logic between digital-based equipment such as power supplies, sensors and actuators that may lead to a digital CCF between and within the defense-in depth echelons. This vulnerability is of particular concern where sensor information is shared between echelons such as the reactor trip system (RTS), engineered safety feature actuation system (ESFAS) and control system as well as indicators used by the operator to establish successful manual control in the mitigation of a postulated event. In other words, all four echelons could be comprised by the same digital CCF due to the sharing of digital sensor output between the echelons.

With this in mind, the equipment and systems in an upgrade package or new reactor design will need to be evaluated to determine which of these components are software based. Examples of some equipment that vendors are currently providing as software based includes:

- Sensors
- Radiation monitors
- Inverters
- Battery chargers
- PPS power supplies
- Breakers including reactor trip breakers (diverse)

This equipment identified as containing EDDs will have to be examined according to the systematic assessment approach defined below.

3.2 Assessment Approach for Treating Potential CCF of Equipment with an EDD

Much of current regulatory guidance on treating CCF vulnerabilities focuses on mitigating the impact of CCF in safety systems (RTS and ESFAS). The prevailing USNRC policy and guidance specifically invokes a consequence-based assessment approach that is primarily applied at the safety system (or redundancy/subsystem) level for sense and command functions. These safety functions are generally characterized as on-demand where the safety action is commanded and executed when indication of an infrequent (transients) or rare (accidents) postulated initiating event (PIE) is sensed. This conventional assessment approach has not been extensively applied at the component level or to equipment whose safety-related function is generally characterized as continuous, frequent, or predictable (such as for many sensing, actuation, and support service equipment).

Because the consideration of CCF vulnerability for equipment with an EDD is a recent regulatory concern and guidance on assessing and addressing potential vulnerabilities is evolving, a systematic approach should be employed to determine when and how a D3 analysis is to be performed for equipment with EDDs. To this end, an assessment approach for systematically evaluating the potential impact of prospective CCF vulnerabilities for equipment with an EDD has been developed by the authors and is described below.

First, the presence of an EDD should be reviewed for each electrical and electronic component evaluated/selected for the implementation of the I&C architecture of an existing or new reactor. To help ensure awareness of EDDs, all specifications to vendors for the supply of safety-related equipment or commercial products should include requirements that any EDD be identified and that sufficient documentation of the quality of any commercial equipment be provided.

If, at any point in the following stages of an assessment of CCF vulnerability of equipment with an EDD, alternate equipment that is determined diverse is found to be available, the I&C architecture can incorporate the diverse equipment as a means of mitigating the impact of potential CCF of the equipment with an EDD. This solution presupposes the result of a conventional D3 analysis to be that diverse means to ensure the safety function supported by the equipment is necessary. If diverse equipment is employed, then the basis for determining that the equipment is diverse should be documented to support justification that the potential impact of CCF is mitigated.

Where equipment with an EDD is identified, the role of the digital device in the performance of any safety-related function either performed or supported by the equipment should be investigated. Where it is determined that the EDD is either not involved in or cannot adversely affect the performance of any safety-related function of the equipment, no further analysis would be necessary but the basis for the determination that the EDD does not impact safety functions should be documented. Where it is determined that the EDD has an impact on the equipment performance or sufficient information on the

role of the EDD is not available, then further assessment of the potential for CCF vulnerabilities should proceed.

In accordance with the approach identified in BTP 7-19 [2], a further aspect of the investigation of the equipment with an EDD involves determination of whether the implementation of relevant functions in the EDD meets either of the two criteria for which it is considered that the potential for CCF is resolved. The first criterion is that there is sufficient internal diversity incorporated in the equipment or the design of the EDD. The second criterion is that the software or software-designed logic is sufficiently simple that it has been or can be fully tested. Assessing the compliance with either criterion requires detailed knowledge of the equipment and the application of the EDD. If either condition can be demonstrated, then no further analysis would be necessary and the basis for this determination should be documented. If the vendor does not provide or have available such information, then further assessment of the potential for CCF vulnerabilities should proceed.

The next stage of the assessment involves evaluating the performance characteristics of the equipment to determine the nature of its failure response. Given that this assessment applies to equipment rather than systems, a key question for the evaluation is whether the equipment performs a function for which failure is self-revealing. For example, if the equipment is continuously or regularly operating (transmitting, maneuvering, controlling), is its failure readily observable? Generally, failure to function of active equipment is apparent. Degraded performance may also give clear, immediate indication. Alternatively, if there is not direct, short-term indication of failure (e.g., failure responses such as “fail as is” or “incorrect but plausible”), then the evaluation should consider whether failure of the equipment can be detected through available or additional monitoring. For example, a sensor output may be plausible but incorrect and, given an assumption of a CCF, comparison against the output of identical sensors could not be expected to reveal the failure. However, comparison against a group of different sensors whose collective behavior is predictable based on physics (i.e., expected process behavior) could detect the failure. Example are seen in monitoring and surveillance capabilities that have been developed for the nuclear power and other industries based on pattern recognition [8]. Thus, potential CCF of equipment with EDDs with continuous, frequent, or predictable behavior may be self-revealing or detectable through surveillance and monitoring techniques.

If the results of the evaluation of the equipment performance characteristics demonstrate that failures are self-revealing or detectable, near-term notification of failure and opportunity to respond rapidly (e.g., restart, transition to a safe state, manual action for reset, bypass, or repair) may provide the means of mitigating the impact of CCF. These conditions should be documented and may be employed as part of a strategy to mitigate the impact of CCF. The additional information necessary to provide justification for such a strategy are the time available for detection and response as well as the response approach itself. The time for detection and response depends on the progression of the event postulated to result from the failure and can be determined through analysis (e.g., conduct of an engineering analysis of appropriate fidelity or proceeding to the best-estimate accident and transient analysis of the conventional D3 analysis). If it is determined that adequate time is available for detection, then a strategy for corrective action (either automatic or manual) should be developed and assessed to ensure that both detection and response can be accomplished in the available time (with margin) before the consequences of a postulated CCF violate applicable acceptance criteria. If it is determined that a “detect and respond” strategy provides adequate mitigation of the impact of CCF, then the strategy itself and the basis for this determination should be documented.

At this stage, the assessment of equipment with an EDD transitions to the conventional D3 analysis. In assessing the impact of a failure of multiple instances of the equipment with an EDD, the context of the architecture, system, redundancy, or subsystem to which it is assigned should be considered. In developing a block representation (as specified in NUREG/CR-6303 [6]) of the I&C architecture, including the software or software designed logic of the EDD, the availability of diverse means to provide the same or similar safety function should be considered. In the specific case of smart sensors, an

evaluation should be performed determine whether a diverse measurement from another dissimilar (diverse) sensor is available. Regarding safety functions, this assessment involves considering the sensor and functional diversity provided in the safety system design to identify whether alternate indicators are incorporated in the plant design for each PIE indicated by the measurement from the smart sensor. If such diversity is present within the safety system block structure, then it may not be necessary to postulate CCF of the equipment. If the measurement from the smart sensor is also shared with the control system echelon, then it would also be necessary to confirm that the anticipated failed behavior of the associated control function is bounded by safety analysis. As is normal in a D3 analysis, documentation should capture the justification that the impact of potential CCF is either mitigated or remains within safety bounds.

If the considerations described in the assessment approach above do not fully resolve the potential impact of CCF in equipment with an EDD, then the equipment should be further treated as part of the conventional D3 analysis (see [2] and [6]). The assessment of equipment with an EDD, including the results of a D3 analysis, are expected to demonstrate that there is sufficient defense-in-depth and diversity to cope with a postulated digital CCF of the EDDs in equipment of the RSS and ESFAS, including the credited control systems.

All of the assumptions and decisions involved in the assessment above and its full execution during the preliminary design of the I&C system architecture of an existing reactor modification or a new reactor implementation should be confirmed as part of a final assessment when the equipment selection,

4 CONCLUSIONS

As noted, nuclear facilities have increased their use and reliance on digital technology in systems and equipment (e.g., I&C, electrical systems, and fluid systems). In addition to digital I&C systems, examples of safety-related equipment that may use digital technology include emergency diesel generators, pumps, valve actuators, motor control centers, breakers, priority logic modules, time-delay relays, and uninterruptible power sources. Because of the high demand for digital functionality in high-volume industries, the industrial I&C marketplace is dominated by digital technology such that it is increasingly difficult to acquire instrumentation that is not equipped with an embedded digital device (EDD) intended to enhance its performance, reliability, and flexibility. Concerns about CCF vulnerability are the primary issue that serves to inhibit deployment of advanced instrumentation (e.g., sensors, actuators, microcontrollers) with EDDs in nuclear power applications.

Regulatory guidance on how to assess equipment with an EDD is very limited. The most direct treatment of EDDs in regulatory information was issued by the USNRC through publication of RIS 2016-05. Specifically, the RIS points to BTP 7-19 as the prevailing guidance for assessing CCF vulnerabilities. However, that guidance focuses on system-level consideration of CCF and does not explicitly address treatment of equipment with an EDD. Therefore, development of targeted methods and approaches is needed to resolve CCF concerns about EDDs and enable the nuclear industry to take advantage of the beneficial capabilities of “smart” equipment.

To this end, the authors have developed an approach for extending the customary D3 analysis to address equipment with an EDD. This approach involves evaluating equipment to ensure awareness of the presence of an EDD, determining the role and safety-relevance of the digital device in the performance of any safety-related function either performed or supported by the equipment, investigating whether the implementation of relevant functions in the EDD meets either of the two criteria (internal diversity or testability) for which it is considered that the potential for CCF is resolved, evaluating the performance characteristics of the equipment to determine the nature of its failure response (e.g., is failure detectable and is adequate time available to respond), assessing whether the component-level CCF has an unacceptable system-level or safety function impact (e.g., performance of a best-estimate analysis), and, if necessary, determination of the availability of diverse alternatives to mitigate the impact of CCF.

In conclusion, international engineering and licensing activities in standards and guidance have been, and are being developed to address this important consideration in protecting safety-related systems. The proposed extended approach to evaluating CCF vulnerability and mitigation in regard to equipment with an EDD can contribute to a more systematic, predictable assessment that can potentially reduce the burden of having to perform a full D3 analysis for every device.

5 REFERENCES

1. U.S. Nuclear Regulatory Commission, "Embedded Digital Devices in Safety-Related Systems," Regulatory Issue Summary 2016-05, April 2016 (ADAMS Accession No. ML15118A015).
2. U.S. Nuclear Regulatory Commission, "Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems," BTP 7-19, Rev. 6, March 2010 (ADAMS Accession No. ML093490771).
3. U.S. Nuclear Regulatory Commission, *Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants*, "Instrumentation and Controls," NUREG-0800, Chapter 7, Rev. 5, Washington, D.C., 2007.
4. U.S. Nuclear Regulatory Commission, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," Staff Requirements Memorandum on SECY-93-087, Washington, D.C., July 21, 1993 (ADAMS Accession No. ML003708056).
5. U.S. Nuclear Regulatory Commission, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," SECY-93-087, Washington, D.C., April 2, 1993 (ADAMS Accession No. ML003708021).
6. U.S. Nuclear Regulatory Commission, *Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems*, NUREG/CR-6303, December 1994 (ADAMS Accession No. ML071790509).
7. U.S. Nuclear Regulatory Commission, "Diversity and Defense-in-Depth (D3) Issues," ISG DI&C-ISG-02, Rev. 2, June 5, 2009 (ADAMS Accession No. ML083310185).
8. Electric Power Research Institute, "On-Line Monitoring Implementation Guidelines: Use of Multivariate State Estimation Technique (MSET)," EPRI 1003360, November 2002.