ORNL/SR-2016/130

Technical Basis for Evaluating Software-Related Common-Cause Failures

Michael Muhlheim
Richard Wood

April 2016

OAK RIDGE NATIONAL LABORATORY
MANAGED BY UT-BATTELLE FOR THE US DEPARTMENT OF ENERGY

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

ORNL/SR-2016/130

Reactor and Nuclear Systems Division

TECHNICAL BASIS FOR EVALUATING SOFTWARE-RELATED COMMON-CAUSE FAILURES

Michael Muhlheim
Richard Wood

Date Published: April 2016

Prepared by
OAK RIDGE NATIONAL LABORATORY
Oak Ridge, TN 37831-6283
managed by
UT-BATTELLE, LLC
for the
US DEPARTMENT OF ENERGY
under contract DE-AC05-00OR22725

CONTENTS

LIST OF FIGURES

ACRONYMS

ADAMS	Agencywide Documents Access and Management System
ALWR	advanced light water reactor
AOO	abnormal operational occurrence
ASIC	Application Specific Integrated Circuit
BDBE	beyond design basis event
BOP	balance of plant
BTP	branch technical position
CCF	common-cause failure
DAS	diverse actuation system
D3	diversity and defense-in-depth
DBE	design basis event
DC	design certification
DI&C	Digital Instrumentation and Controls
DSRS	design-specific review standard
EDG	emergency diesel generator
EFW	emergency feedwater
EPR	US Evolutionary Power Reactor
EPRI	Electric Power Research Institute
ESF	engineered safety feature
ESFAS	engineered safety features actuation system
FSAR	final safety analysis report
GDC	general design criterion
IAEA	International Atomic Energy Agency
I&C	instrumentation and control
ICS	integrated control system
IEEE	Institute of Electrical and Electronics Engineers
IPS	integrated protection system
ISG	interim staff guidance
LSELS	load shedder and emergency load sequencer
MSFIS	main steam and feedwater isolation system
NRC	US Nuclear Regulatory Commission
NSSS	nuclear steam supply system
NUREG	NRC regulatory guide
NUREG/CR	NUREG contractor
NUREG/IA	NUREG international agreement
ORNL	Oak Ridge National Laboratory
PA	postulated accident
PACS	priority and actuator control system
PRA	probabilistic risk assessment
PS	protection system
RCCA	rod cluster control assembly
RPS	reactor protection system
RTS	reactor trip system
RVLIS	reactor vessel level indicating system
SAR	safety analysis report
SAS	safety automation system
SECY	Secretary of the Commission, Office of the NRC
SIL	safety integrity level

SRM	staff requirements memorandum
SRP	standard review plan
SWCCF	software CCF
TC/CCM	thermocouple core cooling monitor
TXS	TELEPERM XS
USAR	updated safety analysis report

ACKNOWLEDGMENTS

The research described in this report was sponsored by the US Nuclear Regulatory Commission (NRC). The findings documented in this report leverage information from prior investigations to capture the basis for regulatory treatment of common-cause failure vulnerability in instrumentation and control systems. In particular, the authors incorporated technical information into this report that was generated through their own prior work under US Department of Energy and NRC Office of Nuclear Regulatory Research sponsorship.

The authors wish to thank the technical peer reviewers and editorial staff at Oak Ridge National Laboratory for their feedback and assistance in improving this report.

Page intentionally blank

EXECUTIVE SUMMARY

The instrumentation and control (I&C) system architecture at a nuclear power plant (NPP) incorporates protections against common-cause failures (CCFs) through the use of diversity and defense-in-depth. Even for well-established analog-based I&C system designs, the potential for CCFs of multiple systems (or redundancies within a system) constitutes a credible threat to defeating the defense-in-depth provisions within the I&C system architectures. The integration of digital technologies into the I&C systems provides many advantages compared to the aging analog systems with respect to reliability, maintenance, operability, and cost effectiveness. However, maintaining the diversity and defense-in-depth for both the hardware and software within the digital system is challenging. In fact, the introduction of digital technologies may actually increase the potential for CCF vulnerabilities because of the introduction of undetected systematic faults. These systematic faults are defined as a "design fault located in a software component" and at a high level, are predominately the result of (1) errors in the requirement specification, (2) inadequate provisions to account for design limits (e.g., environmental stress), or (3) technical faults incorporated in the internal system (or architectural) design or implementation. Other technology-neutral CCF concerns include hardware design errors, equipment qualification deficiencies, installation or maintenance errors, instrument loop scaling and setpoint mistakes.

Title 10, Part 50 of the Code of Federal Regulations (10 CFR 50) does not explicitly address CCFs in I&C systems; however, it does address the individual aspects for mitigating CCFs—independence, diversity, redundancy, qualification, quality assurance, anticipated transient without scram provisions, etc. The general design criterion (GDC) on protection system independence (GDC 22 in 10 CFR 50, Appendix A) identifies "functional diversity or diversity in component design and principles of operation" as design techniques to "be used to the extent practical to prevent loss of the protection function." GDC 21 requires that redundancy and independence be designed into the protection system to assure that no single failure results in the loss of a protection function. However, none of the GDC explicitly address CCF itself or a software failure that affects multiple systems or channels (referred to as software CCFs). Thus, even with diversity and defense-in-depth used to minimize the likelihood and consequences of software CCFs, the concern remains that digital systems are susceptible to CCFs.

The use of diversity and defense-in-depth should minimize the likelihood and consequences of software CCFs. NRC guidance for addressing issues related to diversity and defense-in-depth includes the SRM to SECY 93-087, that requires assessment of defense-in-depth and diversity to demonstrate that vulnerabilities to CCFs have adequately been addressed, and BTP 7-19, that recommends verification of adequate diversity and defense-in-depth in the review of I&C systems. However, the unique characteristics and inherent complexity of digital I&C systems may exacerbate CCF vulnerabilities. Consequently, the traditional strategies for diversity in analog systems—signal, functional, and equipment (e.g., sensor or actuator) diversities—may not be sufficient for digital systems. Similarly, defense-in-depth, which incorporates independent systems at different echelons of defense to compensate for failures in other systems or functions, may have unexpected or unknown dependencies between those echelons.

It is the unexpected or unknown dependencies between echelons that may make digital systems more susceptible to CCFs compared to that of an analog system. During the past 20 years, there have been a significant number of safety-related and important-to-safety digital systems or components installed in operating NPPs. The safety-related digital systems were developed in accordance with the requirements in Appendix B to 10 CFR Part 50 and generally have operated safely. However, ~40% of operating plants have reported potential and actual CCFs in many of these systems. Some CCF vulnerabilities affected a single plant, while others affected several plants using the same digital system.

Because operating experience shows that digital CCFs can and do occur, the adequacy of NRC's current positions on diversity and defense-in-depth was reviewed with a focus on digital (software) applications, their limitations with respect to digital systems, new methods or approaches that could address these limitations, and a determination if any new methods for assessing diversity and defense-in-depth vulnerabilities in digital systems could be implemented within the current guidance.

The following NRC positions related to software CCFs were identified based on an analysis of the SRM to SECY 93-087 and BTP 7-19:

1. consequence-based approach,
2. best estimate analyses,
3. design basis events (DBEs),
4. system/component blocks or function blocks,
5. diversity, and
6. 100% testing.

Each of these positions has positive and negative aspects.

Based on this review the concerns about CCF vulnerabilities for digital I&C systems are still warranted. Design measures can address known vulnerabilities, but diversity remains the primary means for protecting against unknown or unanticipated hazards. The NRC's consequence-based approach to verifying adequate diversity and defense-in-depth in the I&C systems covers software CCFs, which are a subset of the failure modes for the loss of a system. The NRC positions on diversity and defense-in-depth reviewed in this report are inter-related and any changes to the guidance for one may affect another. For example, replacing a consequence-based approach with a risk-informed approach would require significant revisions to the SRM to SECY 93-087 and BTP 7-19; the large uncertainties associated with a risk-informed approach would make any such revisions difficult.

Cyber security vulnerabilities, currently outside the scope of software CCF vulnerabilities, should be evaluated as part of the design and operations of the I&C systems.

1. INTRODUCTION

The US Nuclear Regulatory Commission (NRC) policy on current digital system common-cause failure (CCF) is discussed in (1) the Staff Requirements Memorandum (SRM) to Secretary of the Commission, Office of the NRC (SECY) 93-087, *Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light Water Reactor (ALWR) Designs* [1], and (2) Branch Technical Position (BTP) 7-19, *Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems* [2].

The SRM to SECY-93-087 provides the NRC's four-point position on defense against CCFs in digital instrumentation and control (I&C) systems, and BTP 7-19 presents the NRC position on diversity and defense-in-depth (D3) from the SRM on SECY-93-087. To confirm that the vulnerabilities to CCFs have been adequately addressed, BTP 7-19 recommends verification of the following:

- "adequate diversity has been provided in a design to meet the criteria established by the NRC's requirements,"
- "adequate defense-in-depth has been provided in a design to meet the criteria established by the NRC's requirements," and
- "the displays and manual controls for critical safety functions initiated by operator action are diverse from computer systems used in the automatic portion of the protection systems."

Flawed requirements can be a technology-neutral source of systematic faults that create the potential for CCF vulnerability, and thus can defeat diversity and defense-in-depth measures.

Other sources of common faults that apply to both analog and digital technology that can also defeat diversity and defense-in-depth measures include shared or defective components, fabrication errors, design mistakes, implementation errors, installation errors, operation errors, and maintenance errors.

This report presents a review of the NRC's current technical basis for evaluating software-related CCFs in order to affirm or provide alternatives to the current digital system policy specific to software CCFs.

2. CURRENT NRC POSITION ON SELECTED ISSUES

Based on an analysis of the SRM and Standard Review Plan (SRP) BTP, the following NRC positions on software CCFs were reviewed:

1. consequence-based approach,
2. best estimate analyses,
3. design basis events (DBEs),
4. system/component blocks or function blocks,
5. diversity, and
6. 100% testing.

Each position was evaluated with respect to the following:

- NRC's current position and limitations,
- new methods or approaches that address limitations,
- ability to implement new methods with current guidance, and
- recommendation.

2.1 Consequence-Based Approach

At the NRC Commissioner's briefing on digital I&C, NRC staff members stated that "the current guidance [for evaluating D3] is a consequence-based approach for addressing software common cause failures and does not relate to safety significance. Thus, the same rigor of treatment of software common cause failures is applied to all safety systems without consideration to the significance of the safety function performed by each particular system to overall plant safety" [3].

2.1.1 Current NRC Position and Limitations

Institute of Electrical and Electronics Engineers(IEEE) Standard Criteria for Safety Systems for Nuclear Power Generating Stations (IEEE Std 603-1991) states that safety systems are "relied upon to remain functional during and following design basis events to ensure . . . the capability to prevent or mitigate the consequences of accidents.'' Regulations such as 10CFR50.36, *Technical Specifications*, and the single-failure criterion described in Appendix A, also address the capability to prevent or mitigate the consequences of postulated accidents. Revision 6 of BTP 7-19, which is based on the guidance in NUREG/CR-6303 [4], states that the accidents reviewed are "*occurrences that are not expected to occur but are postulated because their consequences would include the potential for the release of significant amounts of radioactive material*" [emphasis added]. While the regulations specify preventing or mitigating accidents, current guidance is focused on the consequences of accidents, regardless of likelihood, and to the exclusion of any mitigation.

Considering the consequences without considering the likelihood of failure of I&C systems and mitigating capabilities may result in greater overall complexity, increased risk of spurious actuation, more complex specifications and design, modification problems (e.g., maintaining diversity during modification), cost, and the potential lower quality of diverse versions. A deterministic approach requiring the systems to respond to highly unlikely events could lead to designing for diversity where it is not needed. Thus, the impact of the reliability of safety functions to overall plant safety should be reviewed to access potential limitations in current guidance related to diversity and software CCFs.

The deterministic approach of requiring the digital I&C systems to respond to highly unlikely events could lead to design diversity where it is not needed. To address this requires an understanding of the likelihood of an event occurring and the risk that results if an event does occur. However, the resource sharing capabilities for digital systems raises a key concern with respect to reliability, because the use of shared data bases and processing equipment can result in a design that has the potential to propagate a CCF of redundant equipment. That is, a CCF in a digital system can result in loss of defense-in-depth.

2.1.2 New Methods or Approaches that Address Limitations

Revisions to a consequence-based approach for software CCFs may include the frequency for evaluating D3, resulting in risk-informed guidance for system redundancy, independence, and diversity so that systems are maintained commensurate with the expected consequences of challenges to the system. Licensees could consider, among other things, "Whether appropriate restrictions are in place to preclude simultaneous equipment outages that would erode the principles of redundancy and diversity" [5]. Any mitigation of accidents could also be included.

For software, the likelihood of occurrence is based on the assumption that

- a fault (i.e., vulnerability) exists all the time,
- an undetectable trigger event causes a failure, and
- an event occurs that, coupled with the trigger event, results in the loss of a safety function.

An existing fault, as long as it stays dormant, does not affect safety. Its effect on safety cannot be properly assessed without consideration of the conditions that activate the fault to become a failure. The means of activating a fault (i.e., failure vulnerability) is a triggering condition or event. A trigger is a specific event or operating condition that causes an I&C system to fail because of activation of a latent fault. Triggers include plant transients and initiating events, external conditions (e.g., environment, natural phenomena), interactions among systems, human interaction, and internal states (e.g., execution profile, exception handling). A dormant fault in the presence of a trigger becomes an activated fault. The result of an activated fault is a failure.

The probability of a software failure that combines the existing fault and trigger event is difficult to estimate. For software designed to safety integrity level (SIL) 4,[1] the probability of failure on demand is estimated to be 10^{-4} [6]. Although operating experience reviews involving digital I&C systems have shown potential and actual digital I&C CCFs to be unlikely events [7,8,9,10,11], they have not estimated a probability of failure on demand. Operating experience shows that digital CCFs occur, but that they appear to be relatively infrequent.

IEEE Std 7-4.3.2-2003, *Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations*, recognizes that the use of diversity and defense-in-depth are useful in addressing software CCFs. Annex F of this Standard considers the computer as a whole (i.e., hardware, system software, firmware, and applications). The standard notes that “methods that predict software reliability . . . have not yet reached a sufficient state of maturity to provide adequate confidence in the reliability predictions.” NUREG/IA-0463 [6] and operating experience support this.

Latent faults introduced during maintenance from software modifications, setpoint changes, and version revisions in spare parts [12] are a dominant cause of application software failure. In fact, one of the software errors identified by NRC and the Electric Power Research Institute (EPRI) was because of an inconsistency with the system requirements specification [13]. Another event [14] was introduced during the detailed logic design phase of the software development where the designer and independent verifier failed to recognize the interaction between some process logic inhibits and the test logic. Risk-informed guidance rather than consequence-based guidance would not reduce the likelihood of these events. In fact, it could actually increase the likelihood if the events are not considered in the safety assessment.

Risk is measured by the likelihood of an event occurring and its consequence. However, arguments that solely focus on the likelihood part of the risk equation seem to only consider the elimination of diversity and defense-in-depth because of their low likelihood of occurrence. Events with a greater likelihood of occurrence are not considered or evaluated because of their definition as beyond design basis events (BDBEs). For example, probabilistic risk assessments (PRAs) routinely consider BDBEs, some of which are risk significant. As such, the BTP 7-19 approach may ignore some BDBEs that may be significant to safety, resulting in increased complexity and risk in addressing low frequency DBEs.

Although insights can be gained and complexity may be reduced, the state-of-the-art for another limitation is not in the guidance, but it is part of the method for developing and supporting any models. Modeling I&C systems is not sufficiently mature, and there is a lack of software failure data and its associated large uncertainties. Lack of models, data, and the large uncertainties are reasons for taking a deterministic approach to software CCFs.

[1] RG 1.168, Rev. 1, “Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,” states that software used in nuclear power plant safety systems should be assigned safety integrity level 4 (SIL 4) or equivalent.

2.1.3 Ability to Implement New Methods with Current Guidance

In the defense-in-depth philosophy, the NRC recognized that safety cannot be ensured based on any single element of the design, maintenance, or operation of a nuclear power plant. The “expanded use of PRA technology will continue to support the NRC’s defense-in-depth philosophy by allowing quantification of the levels of protection and by helping to identify and address weaknesses or overly conservative regulatory requirements applicable to the nuclear industry.” [15]

Defense-in-depth is applied by providing independent systems at different echelons of defense to compensate for failures in other systems or functions. Diversity is the general approach for addressing perceived vulnerabilities to CCF of I&C system architectures because dissimilarities in technology, function, implementation, etc., can mitigate the potential for common faults. Consequence-based guidance addresses both defense-in-depth and diversity.

The benefits of implementing a consequence-based approach to software CCF include:

- 100% testing does not result in error-free software.
- The uncertainty in estimating the probability that a software CCF exists is large.
- Operating experience has shown that software CCFs do occur.
- A review of digital I&C (DI&C)-related events identified failure modes that are new and unique to digital systems that are not found in older analog systems [16].
- The deterministic approach provides a sufficient margin to allow for new technologies for digital systems and software development.
- The consequence-based approach provides margin to address unknown unknowns.

A limitation of maintaining the consequence-based approach is that the accident analyses provided in Chapter 15 of the safety analysis report (SAR) do not include BDBEs such as software CCFs. The deterministic approach requiring the systems to respond to highly unlikely events could lead to diversity where it is not needed. However, changing from a purely deterministic approach to a probabilistic one may eliminate some sequences from further consideration that may actually increase risk. Conversely, a risk-informed approach may add previously unanalyzed sequences to be evaluated.

Based on the discussion above, the deterministic consequence-based approach is appropriate, and if regulations and guidance are revised, they should include software CCFs (BDBEs) in the accident analyses.

Currently, software CCFs are BDBEs, and their occurrences are not included in the accident analyses. To be included, software CCFs would need to be redefined as a single failure, or the scope of accidents to be evaluated would need to be modified to include software CCFs.

2.1.4 Recommendation

Operating experience shows that software CCFs occur. Events (initiators) may be much more severe or more likely than previously thought and assessing the consequence-based portion of risk (i.e., no consideration of the likelihood of events) addresses the unknown unknowns. Thus, consideration should be given to not only maintaining the consequence-based approach but to actually expanding it to include software CCFs.

2.2 Best Estimate Analyses

Point 2 in the SRM to SECY-93-087 [1] states that "In performing the assessment, the vendor or applicant/licensee should analyze each postulated common-cause failure for each event that is evaluated in the accident analysis section of the safety analysis report (SAR) using best-estimate or SAR Chapter 15 analysis methods. The vendor or applicant/licensee should demonstrate adequate diversity within the design for each of these events."

A concern regarding point 2 from SRP BTP 7-19, Rev. 6 [17] is:

> *The term "best-estimate methods" is more accurately referred to as "realistic assumptions," which are defined as normal plant conditions corresponding to the event. . . . Thus, in performing the assessment, the vendor or applicant should analyze each postulated CCF for each event that is evaluated in the SAR section analyzing power operation accidents at the plant conditions corresponding to the event. This analysis may use realistic assumptions to analyze the plant response to DBEs, or the conservative assumptions on which the Chapter 15 SAR analysis is based.*

2.2.1 Current NRC Position and Limitations

Using a best-estimate approach to demonstrate that vulnerabilities to CCFs have been adequately addressed, the D3 analysis should:

- Analyze the DBEs identified in Chapter 15 of the SAR using best estimates (i.e., realistic assumptions) (BTP 7-19 Point 2).
- If a postulated CCF could disable a safety function that is required to respond to the DBE being analyzed, a diverse means of effective response is necessary (BTP 7-19 Point 3).
- The diverse means for effective responses to the DBE may be through a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions and within the required time (BTP 7-19 Point 3).

A limitation of SRP BTP 7-19 is that it allows for the use of best-estimate methods, but it does not stipulate a need for uncertainty analysis.

For example, in a Chapter 15 accident analysis, the first echelon of defense in BTP 7-19—the non-safety integrated control system (ICS)—is unavailable (i.e., failed). In a D3 assessment, the non-safety ICS can be credited as providing a diverse means for the reactor trip function. In addition, a D3 assessment may take credit for independent manual operator action—the fourth echelon of defense in BTP 7-19. However, clarification regarding Point 4 states that "where the Point 4 displays and controls serve as the diverse means, the displays and controls should be able to function downstream of the lowest-level components subject to the CCF that necessitated the use of the diverse means."

An applicant/licensee's D3 best estimate analysis is reviewed against the acceptance criteria in BTP 7-19 using the detailed guidance of NUREG/CR-6303. The SAR Chapter 15 analyses are performed under conservative assumptions rather than best-estimate assumptions. NUREG/CR-6303 indicates that sometimes a conservative best estimate analysis is used if trip point values are known and if the simulation curves of an incident or a closely similar incident show that alternative reactor parameters exceed trip values. When such information exists, a secondary trip will occur under conservative assumptions. For cases in which secondary trips cannot be clearly determined, it may be necessary to perform simulations that assume the primary trip variable fails. A set of best-estimate (using realistic assumptions) secondary trip sequences for events lacking a clear secondary trip should be deduced or obtained.

Licensees/applicants have used both qualitative and quantitative best estimate analyses.

2.2.1.1 Qualitative best estimate analysis

In the D3 best estimate analysis for Callaway and Wolf Creek, the licensee evaluated the planned replacement of the existing safety and non-safety related I&C systems with digital systems. The analog reactor trip system (RTS) and engineered safety features actuation system (ESFAS) are to be replaced with a digital computer-based reactor protection system (RPS)—the TELEPERM XS (TXS). In addition, as part of the overall I&C upgrade, the non-Class IE l&C systems and the plant computer will also be upgraded using the Siemens process control system—the TELEPERM XP (TXP) [18].

To address the concern that internal failures, including the effects of software errors, will not propagate in such a fashion to defeat safety functions in redundant safety-related channels, Callaway and Wolf Creek performed a best estimate review of the events in the SAR Chapter 15 accident analyses using the guidance in NUREG/CR-6303. In its D3 assessment, all of the events described in final SAR FSAR / updated SAR(USAR) Chapter 15 were selected for *qualitative* reevaluation.

To determine diversity within the different TXS systems (reactor trip system [RTS], ESFAS, and other safety systems), it is partitioned into blocks/modules in accordance with NUREG/CR-6303, Section 2.5 and NUREG-0493. These blocks/modules represent diverse software or equipment/modules. Vulnerability to common-mode failures and diversity within the TXS system is determined at this level. Using the guidance provided in NUREG/CR-6303, the following systems are evaluated for diversity and independence from each other:

- digital-based RTS,
- nuclear steam supply system (NSSS) ESFAS,
- balance of plant (BOP) ESFAS functions,
- other TXS-based safety functions such as
    - the main steam and feedwater isolation system (MSFIS),
    - the emergency diesel generator (EDG) controls,
    - the load shedder and emergency load sequencer (LSELS),
    - Class 1E analog controls,
    - thermocouple core cooling monitor (TC/CCM),
    - the reactor vessel level indicating system (RVLIS), and
    - the qualified display system.

Using a best estimate evaluation methodology, the setpoints of all functions (except those defeated by CCF) are assumed to trip at the actual setpoint rather than at a conservative value such as the analysis limit value. This replaces the conservatism in the SAR Chapter 15 analyses. This implies that the trips and actuations will occur as designed without failures or worse-case allowance for uncertainties within the safety-related instrumentation loops. All control systems except those whose failure initiated the event are considered operable and can aid in the mitigation of the consequences of the event.

The conclusion from the *qualitative* assessment is that the different TXS applications have sufficient diversity to manage postulated software CCFs. The qualitative re-evaluation of FSAR/USAR-analyzed events confirms that sufficient D3 exists in the design of the proposed l&C digital modification to meet the criteria established by the NRC's guidance in BTP 7-19.

The qualitative analysis also concluded that, with respect to the TXS design, at least two independent echelons of defense are provided for each postulated event to protect against postulated yet unlikely software CCF. If a software CCF were to occur, other automatic safety functions and manual system-level actuations would be available to mitigate postulated events.

2.2.1.2 Quantitative best estimate analysis

The method of assessment used for the US Evolutionary Power Reactor (EPR) [19] was to analyze the DBEs analyzed in the SAR Chapter 15 safety analyses, assuming that a software CCF existed in the protection system (PS) and safety automation system (SAS).

The D3 analysis for the EPR uses *quantitative* evaluations of the anticipated operational occurrences (AOOs) and postulated accidents (PAs) in the SAR Chapter 15 accident analyses in the presence of a software CCF that renders the PS ineffective. For a software CCF in the SAS, the only important function identified in the D3 assessment is emergency feedwater (EFW) flow control. A software CCF is evaluated for those events in which EFW is actuated.

The *quantitative* evaluation consists of engineering arguments and engineering analysis to demonstrate that the US EPR I&C design mitigates a software CCF concurrent with an AOO or PA. Realistic assumptions (best estimate) were used.

The computer codes used for this analysis are the same as those used in the safety analysis. Minor changes to the S-RELAP5 computer code were made to reflect improved heat transfer in the steam generator secondary system.

Additionally, the D3 analyses used best estimate modeling assumptions that differed from the US EPR FSAR analysis. The system modeling was changed to reflect available systems and expected behavior during best estimate conditions versus design basis. As an example, consider the uncontrolled rod cluster control assembly (RCCA) withdrawal at power event. This event is defined as the uncontrolled addition of reactivity due to the withdrawal of RCCAs during power operation either due to a failure in an automatic control system or operator error. An SAR Chapter 15 analysis of this event does not credit the ICS for reducing reactor power, whereas the best estimate analysis does (Fig. 1).

The D3 best estimate analysis assesses conformance with Point 2 of SRP BTP 7-19. Frequently, the D3 best estimate analysis entails a quantitative evaluation of the SAR Chapter 15 AOOs and PAs. For example, Fig.1 shows the SAR Chapter 15 conservative analysis (left) [20] and D3 best estimate analysis (right) [21] for an uncontrolled RCCA withdrawal at power and a software CCF in the protection system.

The guidance provided in NUREG/CR-6303 provides a method to identify CCF vulnerabilities and determine if sufficient mitigation is in place. However, as shown above, licensees typically perform analyses that are just as detailed for D3 best estimates as they are for the SAR Chapter 15 accident analyses. In practice, to meet the “necessary to perform simulations that assume the primary trip variable fails” of NUREG/CR-6303 results in the system-based best estimate analyses closely resembling the SAR Chapter 15 accident analyses.

2.2.2 New Methods or Approaches that Address Limitations

In 1979, NUREG-0493 documented the first application of a D3 analysis and identified three echelons of defense. Written 15 years later (1994), NUREG/CR-6303 provides a methodology for conducting a D3 analysis, and it expands the three echelons of defense in NUREG-0493 into four echelons of defense, which were later adopted in SRP BTP 7-19. NUREG/CR-7007 later enhanced the description of diversity types and presented an analysis of the impact of various diversities.

Current guidance allows qualitative and quantitative best estimate analyses. A limitation is the lack of guidance to define the best estimate analysis.

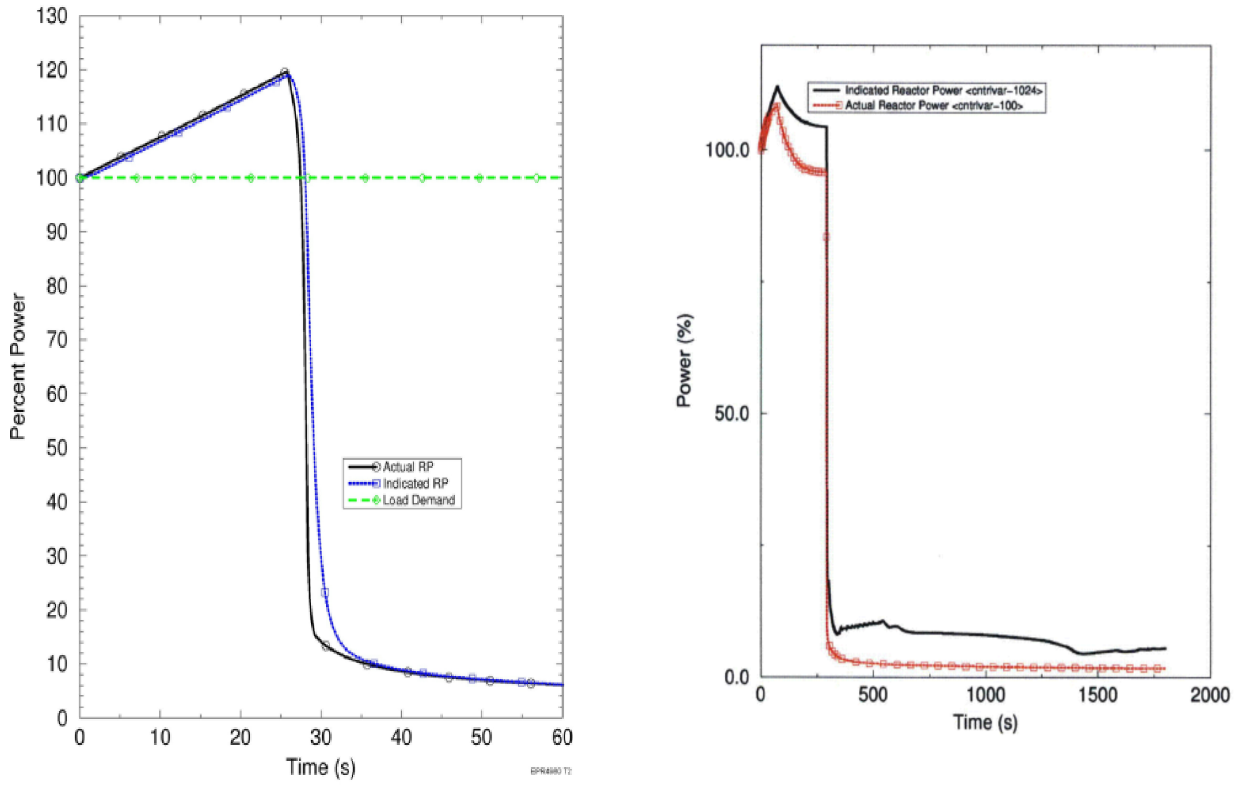

Fig. 1. SAR Chapter 15 conservation analysis (left) and D3 best estimate analysis (right) for an uncontrolled RCCA withdrawal at power and a software CCF in the protection system (Source: US EPR FSAR and ANP 10304).

With the advancements in technology, the use of smart sensors that combine the sensors with a processing unit and a communication interface does not appear to fit into the current D3 assessment guidelines. Therefore, it will be difficult to properly select blocks with smart sensors and with potential CCF vulnerabilities located throughout the system.

2.2.3 Ability to Implement New Methods with Current Guidance

Point 2 in the SRM to SECY-93-087 states that it is acceptable to use best-estimate analyses or SAR Chapter 15 analysis methods. The D3 analyses take the DBAs in SAR Chapter 15 and take credit for non-safety systems. Any analyses are within the scope of best estimates" However, the term *best estimate* may be confusing, because some applicants repeat SAR Chapter 15 analyses, use quantitative analyses that replicate SAR Chapter 15 analyses, or use qualitative analyses based on functions. From a licensing perspective, it appears to the authors of this report that the detailed quantitative analyses seem to be a risk-avoidance approach for D3 best estimate analyses.

2.2.4 Recommendation

NUREG/CR-6303 was based on NUREG-0493. In fact NUREG/CR-6303 includes NUREG-0493 almost verbatim with only slight modifications. Based on this review, it is recommended that NUREG-0493 be added to the Agencywide Documents Access and Management System (ADAMS).

Because NRC has approved both qualitative and quantitative best estimate D3 analyses, the NRC should further define *best estimate* so that licensees know that both approaches are acceptable. The NRC has accepted qualitative and quantitative evaluations. Quantitative evaluations should provide uncertainty analyses.

It is unknown how the advancement of smart sensors would be adequately addressed when using functional blocks in current analyses. This should be explored further by NRC.

2.3 Design Basis Events

DBEs are “Conditions of normal operation, including AOOs, design-basis accidents,[2] external events, and natural phenomena, for which the plant must be designed to ensure functions of safety-related electric equipment that ensures the integrity of the reactor coolant pressure boundary; the capability to shut down the reactor and maintain it in a safe shutdown condition; or the capability to prevent or mitigate the consequences of accidents that could result in potential offsite exposures” [22].

SRP BTP 7-19, Rev. 6 states that

> *the applicant should perform a D3 assessment of the proposed DI&C system to demonstrate that vulnerabilities to CCF have been adequately addressed. In this assessment, the applicant may use realistic assumptions to analyze the plant response to DBEs (as identified in the SAR). If a postulated CCF could disable a safety function that is credited in the safety analysis to respond to the DBE being analyzed, a diverse means of effective response (with documented basis) is necessary*.

A concern regarding point 2 from SRP BTP 7-19, Rev. 6 [17] is:

> *in performing the [D3] assessment, the vendor or applicant should analyze each postulated CCF for each event that is evaluated in the SAR section analyzing power operation accidents at the plant conditions corresponding to the event. This analysis may use realistic assumptions to analyze the plant response to DBEs, or the conservative assumptions on which the Chapter 15 SAR analysis is based*.

2.3.1 Current NRC Position and Limitations

The overall defense in depth strategy of a plant should prevent or mitigate the effects of credible spurious actuations caused by a software CCF that have the potential to place a plant in a configuration not bounded by the plant’s design basis. SRP BTP 7-19 recognizes that “The effects of some credible postulated spurious actuations caused by a software CCF in the automated protection system may not be evaluated in design basis accident analyses. In these cases, an analysis should be performed to determine whether these postulated spurious actuations could result in a plant response that results in conditions that do not fall within those established as bounding for plant design.”

[2] Design Basis Accidents (DBAs) are “Postulated accidents that are used to set design criteria and limits for the design and sizing of safety-related systems and components.” [NUREG-0800, Chapter 15.0]

The dormant fault requires a trigger to become a failure. The conditions under which a postulated software CCF concurrent with events evaluated in the accident analysis section of the SAR are considered BDBEs. The SRM to SECY 93-087 and BTP 7-19 identify software CCF as a BDBE. In the accident analyses, BDBEs are events with a frequency of occurrence $<10^{-4}$/yr. Thus, to include software CCFs in a diversity and defense-in-depth analysis could lead to evaluating events that have a frequency $<10^{-4}$/yr. However, the very low core damage frequency estimates for new reactor designs could lead to many DBEs being dropped from consideration base on their likelihood alone.

When evaluating risk, the risk paradigm is based on high-frequency/low-consequence and low-frequency/high-consequence events. When including risk insights in the definitions of defense-in-depth, it must be noted that risk is dominated by BDBEs, and BDBEs are not always rare events.

NRC's current focus is on analyzing power operating accidents, but other operating states in which risk may not be negligible (i.e., at power, startup/low power, shutdown, and refueling) are not included.

2.3.2 New Methods or Approaches that Address Limitations

A deterministic approach of requiring the systems to respond to highly unlikely events such as software CCFs (BDBEs) could lead to diversity being implemented where it is not needed. However, arguments that focus on the likelihood aspect of the equation seem to only consider the elimination of diversity and defense-in-depth because of its low likelihood of occurrence. Other aspects are not considered in which diversity and defense-in-depth could be beneficial even if the likelihood is greater.

PRAs routinely consider BDBEs, some of which are risk significant. In fact, although risk is dominated by BDBEs, BDBEs are not always rare events [23]. As such, the BTP 7-19 approach may ignore some potentially safety significant sequences that should likely be considered while resulting in increased complexity and risk in addressing low frequency events. Thus, any quantitative screening with respect to defense-in-depth should consider using PRA not only to eliminate events from further consideration, but also to screen in events.

2.3.3 Ability to Implement New Methods with Current Guidance

Software CCFs are BDBEs and are outside the scope of Chapter 15 accident analyses. A limitation to limiting accident analyses to DBEs (and thus eliminating software CCFs from review) is that risk is dominated by BDBEs and that BDBEs are not always rare events. In addition, the Chapter 15 accident analyses focus on power operating accidents, although plant risk may not be negligible in the other plant operating states (i.e., at power, startup/low power, shutdown, and refueling).

The D3 analyses evaluate the DBAs in SAR Chapter 15 by taking credit for the non-safety systems. Risk-informing the selection of events to be analyzed while maintaining an acceptable margin of safety could focus defense-in-depth and diversity attributes where they are needed. However, the very low risk values estimated for the new plant designs could result in many DBEs and BDBEs being screened out from further consideration. Current guidance only addresses power operations and does not address all operating states.

2.3.4 Recommendation

Because risk-informing the selection of DBEs for the D3 analyses may result in many events being screened from consideration, the deterministic selection of events from SAR Chapter 15 analyses should be maintained. In addition, the guidance should be expanded to include all operating states (i.e., at power, startup/low power, shutdown, and refueling).

2.4 System/Component Blocks or Function Blocks

SRP BTP 7-19, Rev. 6 states that "The D3 analysis methods used in ALWR [design certification] DC applications and for operating plant upgrades are documented in NUREG/CR-6303, which describes an acceptable method for performing such assessments."

2.4.1 Current NRC Position and Limitations

Dividing I&C systems into blocks is a systematic way to evaluate the defense-in-depth of a design. The blocks contain groups of components that provide a mechanism for D3 analysis. The system's components and modules are placed within functional units or blocks. NUREG/CR-6303 defines those blocks as "the smallest portion of the system under analysis for which it can be credibly assumed that internal failures, including the effects of software errors, will not propagate to other equipment. The objective of choosing blocks is to reduce the need for detailed examination of internal failure mechanisms while examining system behavior under reasonable assumptions of failure containment." NUREG-0493 defines a block as "a functionally separate group of equipment or software that is (and is in some guidelines required to be) considered as a unit in defense-in-depth analysis."

A D3 assessment necessary to support the defense-in-depth concept of the plant typically decomposes the I&C system into system/subsystem blocks or system functions. The main criterion for selecting blocks based on the guidance in NUREG/CR-6303 is that the actual mechanism of failure inside a block should not be significant to other blocks. Therefore, a block, as defined by NUREG/CR-6303, "is a physical *subset of equipment* and *software* for which it can be credibly assumed that internal failures, including the effects of software errors will not propagate to other equipment or software" [4].

The main criterion for selecting blocks based on the guidance in NUREG/CR-6303 is that "the actual mechanism of failure inside a block should not be significant to other blocks." Examples of typical blocks provided in NRUEG/CR-6303 are computers, local area networks or multiplexers, or PLCs.

As it relates to software, NUREG/CR-6303 states that

> *It is sometimes asserted that two software modules A and B, running in the same computer, are independent by virtue of protection provided by an operating system that controls the access privileges of A and B, or some other non-physical method of separation. This assertion is difficult to defend if it depends upon the reliability of the operating system software that enforces the separation.*

Theoretically, the larger the block size, the simpler the analysis. This would indicate that the analysis should be performed at a functional level. Current practice shows qualitative assessments at the functional level and quantitative assessments at a subsystems and component level. Both types of analyses are used by licensees and have been approved by NRC.

With advancements in technology, the use of smart sensors that are combined with a processing unit, and a communication interface will complicate the definition/application of blocks using the guidance of NUREG/CR-6303.

The difficulty or limitations is in the selection of blocks. The selection of blocks at the component level would necessarily expand to a function level in order to include smart sensors, wireless communications, and demultiplexers/multiplexers within the "sphere of influence" of the software CCF.

Over the years, the situation has changed with new technologies (e.g., PLCs, PLDs), different software coding practices (e.g., the transition from monolithic low-level code to graphically configured function blocks), extensive software engineering and quality assurance standards, and so forth. Because field-programmable gate arrays (FPGAs) are significantly simpler than microprocessors and link only the functions needed for a given application, the complexity of the resulting application system can be significantly less than that of a microprocessor-based system. Also, FPGAs have burned-in programmed logic that reacts to incoming information, and they do not rely on application software continuously running to process incoming information.[3] Thus, FPGAs may be less susceptible than microprocessors to software CCFs.

2.4.2 New Methods or Approaches that Address Limitations

The simplest architecture would consist of a number of independent, redundant channels, each with independent functional systems for control, scram, and engineered safety features (ESFs). Some systems look like this, but in protection systems, for example, the sensors and signal processors may not be separable into functional systems at a subsystem level.

D3 analyses have been performed at the functional level or at a system or subsystem level. More specifically, NUREG-0493 identifies the echelons of defense that perform the scram and ESF safety *functions* for the RESAR-414 integrated control system, whereas NUREG/CR-6303 focuses on *systems/subsystems*.

In order for the defense-in-depth application to be effective, different echelons of defense are used. The combinations of events of concern are, therefore, the concurrent failures of different echelons of defense. This can in principle come about either randomly or causally [24]. The simultaneous random failures of independent echelons of defense are much less likely than the possibility of a causal failure of more than one echelon of defense. That is, the failures in the different echelons of defense are causally related so that their occurrence is not just the random coincidence of multiple independent failures. This causal relationship can arise in a variety of ways, including an incorrect design, a hostile environment (such as fire or flood), incorrect human actions (such as mis-operation), maintenance errors, or a failure in one system inducing failure in another via missiles or power surges. This would include the sharing of corrupted or otherwise incorrect data which are not safely handled (detected and resulting in fail-safe behavior) or cannot be safely handled (cannot be detected, or for which no fail- safe behavior is definable). Thus, shared corrupted or incorrect digital data are not addressed, possibly because functional diversity in the sensor signals would require faulty data from independent, redundant, and diverse sensor types.

NUREG-0493 provides the following examples that explain D3 at a functional level:

> *Defense-in-depth is not provided for every possible postulated failure in the control, scram, or ESF actuation system. For example, if the portion of the ESF actuation system that initiates the emergency core cooling system function were to fail during a loss-of-coolant accident, neither the control system nor the scram system could compensate for such a failure. Rather, the defense-in-depth for this contingency is to be found outside the instrumentation systems, in the piping design, quality assurance, etc., as discussed earlier in this section.*

[3] In this respect, FPGAs are similar to firmware (programmed logic burned in ROM). However, the latter typically originates from software which may therefore be subject to software-related errors.

> *Defense-in-depth is, however, provided within the instrumentation system for many categories of postulated failures. If the control system fails, the scram and ESF actuation systems provide the needed protection. If the scram system fails, the control system forestalls most needs for scram protection, and the ESF actuation system initiates protection for the most probable events involving scram failure. Similarly, if the ESF actuation system fails, the control system and the scram system forestall the need for ESF actuation for most events. The lower probability events that do not have defense-in-depth provided by the control, scram, and ESF actuation systems are taken care of in other ways.*

2.4.3 Ability to Implement New Methods with Current Guidance

The objective of Clause 5.1 of IEEE Std. 603-1991, along with GDCs 21, 23, 24, and 29, is to protect against the loss of a protection or safety *function*.

Point 3 of BTP 7-19 Rev. 6 states that "If a postulated common-mode failure could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common-mode failure, shall be required to perform either the same function or a different function. The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions."

NUREG-0493 states that "The simplest architecture would be a number of independent redundant channels, each with independent functional systems for control, scram, and ESF. Some systems look like this, but the integrated protection system (IPS) does not. The multiple use of signals in the IPS is contrary to the simple control/ scram/ESF architecture, yet it is acceptable in principle . . . . In systems like IPS, then, the sensors and signal processors cannot be separated into functional systems."

Although NUREG-0493 and NUREG/CR-6303 provide different levels of block decomposition for performing D3 assessments, both models provide sufficient evaluations of echelons of defense for D3 assessments. The system and subsystem levels of decomposition are of a finer granularity than the functional level decomposition.

The implementation of the defense-in-depth concept for I&C is achieved mostly at the I&C architectural level [25]. Appendix B of Design-Specific Review Standard DSRS 7.1 provides an approach to describe the I&C system architecture and identifies relevant information to assess the design's conformance to the defense-in-depth concept and the relevant regulations (e.g., 10 CFR 50.55a(h)).

Design or work activities to support and receive approval for cyber security appear to be outside the scope of software CCF vulnerabilities.

2.4.4 Recommendation

Performance of the D3 assessments at the function level should be encouraged. This would minimize (eliminate) the possibility of software errors propagating to other equipment or software, and it should assess advances on technology such as smart sensors and embedded digital devices.

Cyber security vulnerabilities, currently outside the scope of software CCF vulnerabilities, should be evaluated as part of the design and operations of the I&C systems.

2.5 Diversity

NRC Commissioner Peter Lyons provided an historical perspective on CCFs of digital safety system designs in a keynote address to the International Atomic Energy Agency (IAEA) International Conference on CCFs of digital I&C in NPPs [26], stated:

> *First, we often use the term "diversity" and "defense-in-depth" as if they were two separate concepts. However, if defense-in-depth is viewed as the overarching objective, then diversity as well as redundancy and the implicit assumption of independence are three of its most important contributing elements.*

Diversity is the general mitigation approach used for addressing perceived vulnerabilities to CCF of I&C system architectures, because dissimilarities in technology, function, implementation, and so forth, can mitigate the potential for common faults. The diversity approach to ensuring safety uses different (i.e., dissimilar) means to accomplish the same or equivalent function, generally within one functional barrier, to compensate for a CCF that disables one or more echelons of defense. Diversity is complementary to the principle of defense-in-depth, and it increases the chances that defenses at a particular level or depth will be actuated when needed. Defenses at different levels of depth may also be diverse from each other.

Diversity is one of the design attributes used to eliminate consideration of CCF (the other is testing, as described below). If sufficient diversity exists in the protection system, then the potential for CCF within the channels can be considered to be appropriately addressed without further action.

Point 3 in the SRM to SECY-93-087 states that "If a postulated common-cause failure could disable a safety function, a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common-cause failure, should be required to perform either the same function as the safety system function that is vulnerable to common-cause failure or a different function that provides adequate protection. The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions."

2.5.1 Current NRC Position and Limitations

The defense-in-depth approach to ensuring safety employs different functional barriers to compensate for failures in any one or more of the lines of defense. For I&C systems, diversity embodies the principle of sensing different parameters using different technologies, different logic or algorithms, or different actuation means to provide several ways of detecting and responding to an event. Diversity is the general mitigation approach used for addressing perceived vulnerabilities to CCF of I&C system architectures, because dissimilarities in technology, function, implementation, and so forth can mitigate the potential for common faults. The diversity approach to ensuring safety uses different (i.e., dissimilar) means to accomplish the same or equivalent function, generally within one functional barrier, to compensate for a CCF that disables one or more echelons of defense. Thus, diversity is complementary to the principle of defense-in-depth, and it increases the chances that defenses at a particular level or depth will be actuated when needed. Defenses at different levels of depth may also be diverse from each other.

NUREG/CR-6303 separates the diversity attributes into the following six areas (compared to four in NUREG-0493) to facilitate assessments of adequate diversity in safety systems:

1. **human [life-cycle] diversity:** separate designers, different maintenance personnel on redundant systems,
2. **design diversity:** the use of different approaches, including both software and hardware, to solve the same or similar problem,
3. **software [logic] diversity:** the use of different programs designed and implemented by different development groups with different key personnel to accomplish the same safety goal,

4. **functional diversity:** using different parameters, different technologies, different logic or algorithms, or different actuation means to provide several ways of detecting and responding to a significant event,
5. **signal diversity:** the use of different sensed parameters to initiate protective action in which any of the parameters may independently indicate an abnormal condition, even if the other parameters fail to be sensed correctly,
6. **equipment [manufacturer] diversity:** the use of different equipment to perform similar safety functions, in which *different* means sufficiently unlike as to significantly decrease vulnerability to common failure).

The guidance in NUREG/CR-6303 provides a set of recommended criteria for each of the six diversity attributes, with several diversity criteria within each attribute. However, because of the number of criteria in each attribute is 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.

There may be consequences in factoring in too much diversity in the design or making the systems too complicated in their operation or maintenance. Increased diversity may also affect training and knowledge about the system and individual parts. As recognized by ACRS member Maynard, “we can make it where it is so complicated it becomes less safe than if we had less diversity or less defense-in-depth sometimes. So we have to find that right balance . . . . There are consequences for being too conservative. And there are consequences for not being conservative enough” [27]. The following observations are made related to the too much/too little diversity:

- CCF vulnerabilities still exist. It is believed that the likelihood of finding CCF vulnerabilities is greater because of increased awareness and reviews and thus the number is smaller.
- Potential CCF vulnerabilities will be more complicated and more difficult to identify as system complexity increases.
- If a diverse actuation system (DAS) increases the number of transients, it directly increases plant risk.
- Addressing D3 concerns could actually increase system complexity, fidelity, interactions/vulnerabilities between systems/trains, and number of transients.

2.5.2 New Methods or Approaches that Address Limitations

In NUREG/CR-7007, the human diversity attribute in NUREG/CR-6303 is designated as the life-cycle diversity attribute to account for its true nature and to avoid the erroneous implication that this attribute involves plant operator diversity or human-versus-machine diversity. Additionally, the single equipment diversity attribute in NUREG/CR-6303 is treated as two diversity attributes: *equipment manufacturer* and *logic processing equipment*. Finally, the software diversity attribute is designated as the logic diversity attribute to account for the different means of representing and executing functions that diverse technologies provide, such as software for microprocessors, hardwired logic in programmable devices, or electronic circuitry for analog modules.

The classification of diversity strategies developed in NUREG/CR-7007 consists of three families of strategies: (1) Strategy A, different technologies, (2) Strategy B, different approaches within the same technology, and (3) Strategy C, different architectures within the same technology. Even with D3 used to minimize the likelihood of software CCFs, the concern remains that digital systems are susceptible to a

CCF. During the past 20 years, a significant number of safety-related and important-to-safety digital systems or components have been installed in operating NPPs. The safety-related digital systems were developed in accordance with the requirements in Appendix B to 10 CFR Part 50 and generally have operated safely. However, 38 out of approximately 100 operating plants have reported potential and actual CCFs in many of these systems. Some CCFs affected a single plant, while others affected several plants using the same digital system.

Thus, the use of probabilistic/risk insight to deal with DBEs and BDBEs may be insufficient for ensuring safety, indicating that diversity is still necessary.

2.5.3 Ability to Implement New Methods with Current Guidance

SRP BTP 7-19 endorses NUREG/CR-6303. NUREG/CR-7007 provides a more complete discussion of diversity and its attributes. The strategies provided in NUREG/CR-7007 should be coupled with the blocks in NUREG/CR-6303. The guidance in BTP 7-19 should be revised to include this.

2.5.4 Recommendation

The way to measure diversity is through consequence-based assessments, best-estimate analyses, evaluation of DBEs (and BDBEs), and qualitative or quantitative function block analyses; all are essentially consequence-based assessments.

If a systems-based approach is to be used, the guidance in BTP 7-19 should be revised to endorse the strategies in NUREG/CR-7007 when selecting blocks using the guidance in NUREG/CR-6303.

2.6 100% Testing

With respect to testability, SRP BTP 7-19, Rev. 6 states that

> *If a portion or component of a system can be fully tested, then it can be considered not to have a potential for software-based CCF. Fully tested or 100% testing means that every possible combination of inputs and every possible sequence of device states are tested, and all outputs are verified for every case.*

2.6.1 Current NRC Position and Limitations

The measures necessary for the defense against software CCF include more than testing. Thus, the question of whether 100% testing is sufficient to conclude that the likelihood of a software CCF is sufficiently low cannot be addressed without understanding its place in the development process. The measures for defense against software CCFs are development, testing, and analyses.

2.6.1.1 100% Testing or 100% Combinatorial Testing

Although the statement regarding 100% testing may seem self-explanatory, the two cases below show that there are different interpretations of "*100% testing*." The first example uses 100% combinatorial testing, while the second uses 100% testing.

1. Technical Report ANP-10304 for the EPR [28] states that "100 percent combinatorial testing demonstrates that the priority modules in Priority and Actuator Control System (PACS) are not subject to SWCCF [software CCF]." Accordingly, NRC staff members did not require a demonstration of the D3 plant response conformance to the guidance of SRP BTP 7-19 for a postulated CCF of the priority actuation and control system (PACS) priority module. Thus, based on the applicant's commitment to 100 percent combinatorial testing of the PACS, NRC staff

members determined that the PACS does not need to be considered for a postulated software CCF within the applicant's D3 analysis [29]. The 100 percent combinatorial testing demonstrates sufficient quality of the logic such that a software CCF of the device would be of a *sufficiently low frequency* that it would not need to be considered in the D3 design. The NRC stated that "Based on the commitments for 100 percent combinatorial testing, the staff finds the PACS design meets IEEE Std 603-1998, Clause 5.16 and GDC 22" [29].

2. The Application Specific Integrated Circuit (ASIC)-Based Replacement Module by Westinghouse [30] is assembled from logic blocks. Before they were assembled, the logic blocks were tested to confirm that they perform as required. The logic blocks were then added one at a time. Each time a block was added, tests were performed to confirm that the new block performed as required. After all of the circuits in the ASIC were assembled, Westinghouse performed functional and design testing to verify that the ASIC design and fabrication were both correct. For functional testing, Westinghouse used a set of test vectors to determine whether each of the eight independent circuits in the ASIC was operating properly to show that each of the circuits was correctly designed. Fabrication testing exercised nodes in the ASIC to determine whether the manufacturing process resulted in any faulty components in the ASIC. For these tests, Westinghouse used two sets of test vectors totaling 225,000 test vectors. These tested 100 percent of the functions and exercised 99.8 percent of the nodes. Based on the ASIC development and the 225,000 test vectors that covered 100 percent of the functions and 99.8 percent of the nodes, the NRC staff members concluded that Westinghouse successfully validated the identified critical characteristic through testing. Therefore, the ASIC was determined to satisfy the *quality requirements* of 10 CFR Part 50 Appendix B through application of the guidance in EPRI TR-102348.

100 percent (combinational) testing and manual verification is used to provide assurance on the *quality* of the software development process and addresses the *likelihood* of a software CCF.

Testing is a vital aspect of every development, not only because it exposes flaws, but also because it provides feedback on the quality of the development process. The use of a high quality software development process such as that provided in SRP BTP 7-14 is a design feature that prevents or limits the effects of hardware and software failures, i.e., development techniques that minimize the possibility of mistakes or reduce the consequences of errors. A high quality software development process reduces the likelihood of software failures.

"Software . . . fails because of bugs: errors in the code that cause a program to fail to meet its specification. In fact, only a tiny proportion of failures can be attributed to bugs. . . by far the largest class of problems arises from errors made in the eliciting, recording, and analysis of requirements" [31]. Thus, a limitation in current guidance is the uncertainty or confusion of 100% testing for updated or modified software.

2.6.1.2 Development

IEC 60880 states that "high-quality software engineering practices are the most important defense against software CCF" [32]. NRC's quality assurance requirements and guidance related to the software development process for software in safety systems include the following:

- 10 CFR Part 50, Appendix B, requires a quality assurance program that meets the quality requirements (design, qualification, quality, etc.) applicable to safety-related hardware or software.
- Clause 5.16 in IEEE Std 603 (added in the IEEE Std 603-2006 version), and IEEE Std 7-4.3.2-2003 provide guidance on performing an engineering evaluation of software CCFs, including use

of manual action and non-safety-related systems, components, or both, to provide a means to accomplish the function that would otherwise be defeated by the CCF.

- RGs 1.168−1.173 [33, 34, 35, 36, 37, 38] provide guidance for the development and inspection of software throughout the life-cycle process.
- SRP BTP 7-14 [39] provides guidance on the NRC staff's acceptance of software for safety system functions that is based on (1) confirmation that acceptable plans were prepared to control software development activities, (2) evidence that the plans were followed in an acceptable software life cycle, and (3) evidence that the process produced acceptable design outputs. This BTP provides guidelines for evaluating software life-cycle processes for digital computer-based I&C systems.
- DI&C-Interim Staff Guidance (ISG)-04, Rev. 1 states that "Adequate configuration control measures should be in place to ensure that software-based priority modules that might be subject to software CCF will not be used for credited diversity" [40].

The development process starts with the specifications and requirements. However, if the specification is incorrect, 100% testing is not equivalent to error-free software.

Related to this is that anticipating all combinations of malfunctions may not be possible in a software controlled system, meaning that achieving complete safety may be impossible.

2.6.1.3 Analyses

The analyses part of the measures for defense against software CCFs is missing from current guidance. Even if its correctness has been proven mathematically via analyses, no software system can be regarded as dependable[4] if it has not been extensively tested. A conventional definition of software reliability is "the probability that software will not fail in a specified period of time. [41] Dependability is defined as the "trustworthiness of a delivered service (e.g., a safety function) such that reliance can justifiably be placed on this service [42]." Attributes of dependability include reliability, availability, and safety. Testing and analyses are complimentary and overlap. "Because the activities of testing differ so markedly from those involved in analysis, testing provides important redundancy and can identify mistakes made during the analysis process. Testing can find flaws that elude analysis because it exercises the system in its entirety, whereas analyses typically make assumptions about the execution platform that may not be unwarranted [31]."

2.6.2 New Methods or Approaches that Address Limitations

While software CCFs are possible, their relative frequency of occurrence is thought to be lower than other sources of observed CCFs. This is likely because the software development process, testing, and analyses results in the development of high quality software. Operating experience provides further confidence in the dependability of the software. However, the continual onset of obsolescence of digital systems can limit the amount of experience that can be gained from the use of a specific component (including software) or application over a longer period, thereby diminishing the value of reviewing operating experience. Coupled to this is that one of the dominant causes of application software failure is latent faults introduced during maintenance because of software modifications, setpoint changes, and version revisions in spare parts. Thus, continually updating system software increases the likelihood of a latent fault in that software.

While testing can be used to identify faults, it does not eliminate the possibility that a fault exists. Even if one tests ALL the requirements via a robust testing program, that fact in itself is no guarantee of a

[4] Attributes of dependability include reliability, availability, and safety.

flawless or perfect system. “100% testing of the requirements is no guarantee of flawless system performance” [43]. That is, testing can reveal the presence of errors but not their absence. Thus, 100% testing does not eliminate software CCF concerns.

Per NRC’s current guidance, 100% testing of a software-based device allows that device to be treated as a hardware only device not susceptible to a software CCF [43].

The 100% combinational testing and manual verification provides assurance on the quality of the software development process and addresses the likelihood of a potential software CCF being introduces in the design development process. The 100% testing does not eliminate potential design faults that may be introduced in the requirements specification or design specification phases of the development lifecycle nor prove the absence of CCFs as they could still occur from sources such as potential design faults that may be introduced in the requirements specification or design specification phases of the development lifecycle, hardware design errors, or improper maintenance. [29, 43] However, the goal of the guidance to address all CCFs was “to reduce the likelihood of software CCFs to such a level that the device could be treated, from a regulatory perspective, similar to analog equipment.” [43]

However “Even if the verification and validation program for a given system provides 100% testing coverage, there is no guarantee that the testing is all-encompassing or exhaustive for real-world conditions. Even if one tests ALL the requirements via a robust testing program, that fact in itself is no guarantee of a flawless or perfect system. 100% testing of the requirements is no guarantee of flawless system performance” [43]. That is, testing can reveal the presence of errors but not their absence. Thus, 100% testing without a high quality development process, supplemented with sufficient analyses, does not fully address the software CCF concerns.

Testing cannot identify all the defects within software.

Not all software defects are caused by coding errors. One common source of expensive defects is requirement gaps, e.g., unrecognized requirements which result in errors of omission by the program designer [44].

Combing pairs of combinations together at least once (100% combinatorial testing) during the testing process can significantly reduce the number of tests compared to testing every combination (100% testing).

In the SE for the EPR, the NRC staff stated that “Overall, the staff finds that the Priority and Actuator Control System logic development using 100 percent combinatorial testing satisfies the guidance in DI&C ISG-04 and, therefore, meets the requirements of IEEE Std 603-1998, Clause 5.3.”

2.6.3 Ability to Implement New Methods with Current Guidance

The current guidance has resulted in different interpretations of what constitutes 100% and implementation of testing requirements. For example, is *100% testing* defined as 100% testing of each individual function, or is it 100% testing of the combinations thereof? Can modules be individually 100% tested and then combined? Do new software development methods lessen the 100% testing criterion?

The design attributes of *sufficient diversity* and *testability* can be used to eliminate consideration of CCF. However, current guidance to address software CCFs focuses on testing without coupling it to the development process and analyses. Thus, it should be noted that:

- 100% testing assumes that the software was developed using a quality development process,
- 100 percent testing does not prove the absence of CCFs,

- testing can reveal the presence of errors but not their absence, and
- analyses should show that the unavailability or spurious operation of the actuated device is accounted for in or bounded by the plant safety analysis.

2.6.4 Recommendation

Although the statement regarding "100% testing" may seem self-explanatory, there are different interpretations of "*100% testing*"—is it 100% combinatorial testing, or is it 100% testing. A limitation of 100% testing is that 100% testing is not equivalent to error-free software nor does it prove the absence of CCFs. Another limitation of the current guidance (in addition to the confusion of the meaning of 100% testing) is that the current guidance to address software CCFs focuses on testing without coupling it to the development process and analyses.

100% testing should always be coupled to a quality development process. 100% combinatorial testing and 100% testing should be addressed in guidance documents or in a positon paper.

3. RECOMMENDATIONS

Because operating experience shows that digital CCFs can and do occur, the adequacy of NRC's current positions on diversity and defense-in-depth was reviewed with a focus on digital (software) applications, their limitations with respect to digital systems, new methods or approaches that could address these limitations, and a determination if any new methods for assessing diversity and defense-in-depth vulnerabilities in digital systems could be implemented within the current guidance.

Each of the NRC's positions related to software CCFs were identified based on an analysis of the SRM to SECY 93-087 and BTP 7-19, has positive and negative aspects:

1. Consequence-Based Approach: The use of a consequence-based approach may result in greater overall system complexity and superfluous diversity, but it provides margin to allow for new technologies, and when combined with best estimate analyses, addresses potential software CCFs. A limitation in the current consequence-based approach is that software CCFs, which are BDBEs, are not specifically included in the analyses.
2. Best Estimate Analyses: Typical best estimate analyses using the guidance of NUREG/CR-6303 are quantitative assessments that resemble SRP Chapter 15 accident analyses in complexity. Qualitative reviews, similar to consequence-based assessments, assume the failure of those functions defeated by the CCF under consideration. Unlike the consequence-based approach, a best estimate analysis considers all control systems as available except those whose failure initiated the event. An advantage of qualitative best estimate analysis based on functions is that it encompasses software CCFs.
3. Design Basis Events (DBEs): SRP BTP 7-19 recognizes that "The effects of some credible postulated spurious actuations caused by a software CCF in the automated protection system may not be evaluated in design basis accident analyses." This is because software CCFs are BDBEs and are outside the scope of Chapter 15 accident analyses. A limitation to limiting accident analyses to DBEs (and thus eliminating software CCFs from review) is that risk is dominated by BDBEs and that BDBEs are not always rare events. In addition, the Chapter 15 accident analyses focus on power operating accidents, although other operating states in which risk may not be negligible (i.e., at power, startup/low power, shutdown, and refueling) are included in PRAs.

4. System/Component Blocks or Function Blocks: Dividing I&C systems into blocks using the guidance of NUREG/CR-6303 is a systematic way to evaluate the defense-in-depth of a design. The blocks contain groups of components that provide a mechanism for diversity and defense-in-depth analysis. Theoretically, the larger the block size, the simpler the analysis. Qualitative analyses performed at a functional level mimic the consequence-based approach/qualitative best-estimate analyses. Quantitative assessments are performed at a subsystems and component level. Performance of the diversity and defense-in-depth assessments at the function level should be encouraged; this would minimize (eliminate) the possibility of software errors propagating to other equipment or software. It is unknown if the advancement of smart sensors or embedded digital devices would be adequately addressed when using function blocks based on current guidance; this affects consequence-based and best-estimate analyses and should be explored further by NRC.
5. Diversity: Diversity is one of the design attributes used to eliminate consideration of CCFs (the other is testing). If sufficient diversity exists in the protection system, then the potential for CCFs within the channels can be considered to be appropriately addressed without further action. The diversity approach to ensuring safety uses different (i.e., dissimilar) means to accomplish the same or equivalent function, generally within one functional barrier, to compensate for a CCF that disables one or more echelons of defense. As recognized by ACRS member Maynard, "There are consequences for being too conservative. And there are consequences for not being conservative enough." The way to measure diversity is through consequence-based assessments, best-estimate analyses, evaluation of DBEs (and BDBEs), and qualitative or quantitative function block analyses; all are essentially consequence-based assessments.
6. 100% testing: SRP BTP 7-19, Rev. 6 states that "*Fully tested or 100% testing means that every possible combination of inputs and every possible sequence of device states are tested, and all outputs are verified for every case.*" Although the statement regarding "100% testing" may seem self-explanatory, there are different interpretations of "*100% testing*"—is it 100% combinatorial testing, or is it 100% testing. A limitation of 100% testing is that 100% testing is not equivalent to error-free software nor does it prove the absence of CCFs. Another limitation of the current guidance (in addition to the confusion of the meaning of 100% testing) is that the current guidance to address software CCFs focuses on testing without coupling it to the development process and analyses.

Based on this review the concerns about CCF vulnerabilities for digital I&C systems are still warranted. Design measures can address known vulnerabilities, but diversity remains the primary means for protecting against unknown or unanticipated hazards. The NRC's consequence-based approach to verifying adequate diversity and defense-in-depth in the I&C systems covers software CCFs, which are a subset of the failure modes for the loss of a system. The NRC positions on diversity and defense-in-depth reviewed in this report are inter-related and any changes to the guidance for one may affect another. For example, replacing a consequence-based approach with a risk-informed approach would require significant revisions to the SRM to SECY 93-087 and BTP 7-19; the large uncertainties associated with a risk-informed approach would make any such revisions difficult.

Cyber security vulnerabilities, currently outside the scope of software CCF vulnerabilities, should be evaluated as part of the design and operations of the I&C systems.

4. REFERENCES

1. SRM on SECY-93-087, “Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs,” July 21, 1993 (ADAMS Accession No. ML003708056).
2. BTP 7-19, Rev. 6, “Guidance for Evaluation of D3 in Digital Computer-Based Instrumentation and Control Systems,” US NRC, July 2012 (Adams Accession No. ML110550791).
3. [Commissioner’s] Briefing on Digital Instrumentation and Control, Thursday, December 17, 2015.
4. US Nuclear Regulatory Commission, *Method for Performing D3 Analyses of Reactor Protection Systems*, NUREG/CR-6303, December 1994.
5. SRP 16.0, Rev. 3, “Technical Specifications,” March 2010.
6. S. Birla, R. Sydnor, and N. Carte, *(Availability of) An International Report on Safety Critical Software for Nuclear Reactors by the Regulator Task Force on Safety Critical Software (TF-SCS)*, NUREG/IA-0463, December 2015.
7. R. Torok, EPRI Project Manager, “Benefits and Risks Associated with Expanding Automated Diverse Actuation System Functions,” May 16, 2008 (Adams Accession No. ML090860465).
8. “Assessment of Digital System Operating Experience Data and System Inventory and Classification Structure” (Adams Accession No. ML080590323).
9. J. H. Bickel, “Risk implications of digital reactor protection system operating experience,” Evergreen Safety and Reliability Technologies, LLC., Evergreen, Colorado.
10. http://www.nrc.gov/about-nrc/regulatory/research/digital/faqs.html.
11. EPRI, *Operating Experience Insights on Common-Cause Failures in Digital Instrumentation and Control Systems*, EPRI 1016731, Final Report, December 2008.
12. R. T. Wood, et. al., *Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems*, NUREG/CR-7007, December 2008.
13. LER 529/2005-004, R00, “Technical Specification Required Shutdown Due to Core Protection Calculators Inoperable,” issued October 10, 2005.
14. LER 250/94-005-01, “Design Defect in Safeguards Bus Sequencer Test Logic Places Both Units Outside the Design Basis,” Event Date: 11/03/94, Report Date: 07/17/95.
15. U.S. Nuclear Regulatory Commission, “Policy Statement on Use of Probabilistic Risk Assessment Methods in Nuclear Regulatory Activities; Final Policy Statement,” Federal Register, Vol. 60, No. 158, pg. 42622-42629, August 16, 1995.
16. K. Korsah et. al., *An Investigation of Digital Instrumentation and Control System Failure Modes*, ORNL/TM- 2010/32, March 2010.
17. BTP 7-19, Rev. 6, “Guidance for Evaluation of D3 in Digital Computer-Based Instrumentation and Control Systems,” US NRC, March 2010 (ML093490771).
18. “Callaway Plant and Wolf Creek Generating Station Defense-in-Depth And Diversity Assessment,” 51-502459101, FRAMATOME ANP (ML040720440).
19. Technical Report ANP-10304, Revision 5, “US EPR Diversity and Defense-in-Depth Assessment,” AREVA NP Inc., May 2012.

20. Areva NP, *US EPR Final Safety Analysis Report*, Chapter 15.4, “Reactivity and Power Distribution Anomalies” (ML13073A787).

21. Technical Report ANP-10304, Revision 5, “US EPR Diversity and Defense-in-Depth Assessment,” AREVA NP Inc., May 2012.

22. NUREG-0800, *Standard Review* Plan, Chapter 15.0, “Introduction - Transient And Accident Analyses,” March 2007.

23. Fleming, K.N., and Silady, F.A., “A Risk Informed Defense-in-Depth Framework for Existing and Advanced Reactors,” *Reliability Engineering & System Safety*, Volume 78, issue 3, December 2002, Pg 205-225.

24. NUREG-0493, A Defense-in-Depth and Diversity Assessment of the RESAR-414 Integrated Protection System, US NRC, March 1979.

25. DSRS 7.1, Appendix B, “Fundamental Design Principles.”

26. Dr. Peter B. Lyons, Commissioner, US Nuclear Regulatory Commission, “Keeping the ‘Safe’ in New Digital Safety System Designs,” Keynote Address to the IAEA International Conference on Common-Cause Failures of Digital Instrumentation and Control Systems in Nuclear Power Plants, S-07-028, June 19, 2007.

27. Advisory Committee on Reactor Safeguards Subcommittee on Digital Instrumentation and Control Systems, Wednesday, April 18, 2007.

28. ANP-10304, Rev. 5, “US EPR Diversity and Defense-in-Depth Assessment,” AREVA NP Inc., May 2012 (ML12157A120).

29. “Safety Evaluation with Open Items US EPR Design Certification Chapter 7 – Instrumentation and Control Systems” (ML090780501).

30. Safety Evaluation by the Office of Nuclear Reactor Regulation Westinghouse Electric Company Topical Report WCAP-15413, “Westinghouse 7300a ASIC-Based Replacement Module Licensing Summary Report.”

31. D. Jackson, M. Thomas, and L. I. Millett, Editors, *Software for Dependable Systems: Sufficient Evidence?*, The National Academies Press, 2007.

32. IEC 60880, “Nuclear power plants-Instrumentation and control systems important to safety—Software aspects for computer-based systems performing Category A functions,” February 2005.

33. RG 1.168, Rev. 2, “Verification, Validation, Reviews, And Audits For Digital Computer Software Used In Safety Systems Of Nuclear Power Plants,” July 2013.

34. RG 1.169, Rev. 1, “Configuration Management Plans for Digital Computer Software Used In Safety Systems of Nuclear Power Plants,” July 2013.

35. RG 1.170, Rev. 1, “Software Test Documentation for Digital Computer Software Used In Safety Systems of Nuclear Power Plants, July 2013.

36. RG 1.171, Rev. 1, “Software Unit Testing for Digital Computer Software Used In Safety Systems of Nuclear Power Plants,” July 2013.

37. RG 1.172, Rev. 1, “Software Requirements Specifications for Digital Computer Software Used In Safety Systems of Nuclear Power Plants,” July 2013.

38. RG 1.173, Rev. 1, “Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,” July 2013.

39. SRP BTP 7-15, Rev. 5, “Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems,” March 2007.

40. DI&C-ISG-04, Rev. 1, “Digital Instrumentation and Controls,” March 6, 2009 (ML083310185).

41. K. W. Miller et. al., “Estimating the Probability of Failure When Testing Reveals No Failures,” *IEEE Transactions on Software Engineering*, Vol. 18, No. 1, January 1992.

42. B. Littlewood et al., “DISPO Project at City University,” Centre for Software Reliability, City University, London, 2006.

43. SECY-15-0106, Enclosure 7, “Position Paper on Staff Update to 10 CFR 50.55a(h) Rule Affecting I&C Systems” (ML14281A145).

44. Kolawa, Adam; Huizinga, Dorota (2007). Automated Defect Prevention: Best Practices in Software Management. Wiley-IEEE Computer Society Press. p. 426. ISBN 0-470-04212-5.