U.S. NUCLEAR REGULATORY COMMISSION

STANDARD REVIEW PLAN

BRANCH TECHNICAL POSITION 7-19

GUIDANCE FOR EVALUATION OF POTENTIAL COMMON CAUSE FAILURE DUE TO LATENT SOFTWARE DEFECTS IN DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS

REVIEW RESPONSIBILITIES

Primary – Organization responsible for the review of instrumentation and controls (I&C)

Secondary – Organization responsible for the review of reactor systems and the organization responsible for the review of human factors engineering (HFE)

Review Note: The revision numbers of regulatory guides (RGs) and the years of endorsed industry standards referenced in this branch technical position (BTP) are centrally maintained in NUREG-0800, “Standard Review Plan for the Review of Safety Analysis Reports for Nuclear

Draft Revision 8 – November 2019

USNRC STANDARD REVIEW PLAN

This Standard Review Plan, NUREG-0800, has been prepared to establish criteria that the U.S. Nuclear Regulatory Commission staff responsible for the review of applications to construct and operate nuclear power plants intends to use in evaluating whether an applicant/licensee meets the NRC's regulations. The Standard Review Plan is not a substitute for the NRC's regulations, and compliance with it is not required. However, an applicant is required to identify differences between the design features, analytical techniques, and procedural measures proposed for its facility and the SRP acceptance criteria and evaluate how the proposed alternatives to the SRP acceptance criteria provide an acceptable method of complying with the NRC regulations.

The standard review plan sections are numbered in accordance with corresponding sections in Regulatory Guide 1.70, "Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants (LWR Edition)." Not all sections of Regulatory Guide 1.70 have a corresponding review plan section. The SRP sections applicable to a combined license application for a new light-water reactor (LWR) are based on Regulatory Guide 1.206, "Combined License Applications for Nuclear Power Plants (LWR Edition)."

These documents are made available to the public as part of the NRC's policy to inform the nuclear industry and the general public of regulatory procedures and policies. Individual sections of NUREG-0800 will be revised periodically, as appropriate, to accommodate comments and to reflect new information and experience. Comments may be submitted electronically by email to NRO_SRP@nrc.gov.

Requests for single copies of SRP sections (which may be reproduced) should be made to the U.S. Nuclear Regulatory Commission, Washington, DC 20555, Attention: Reproduction and Distribution Services Section, or by fax to (301) 415-2289; or by email to DISTRIBUTION@nrc.gov. Electronic copies of this section are available through the NRC's public Web site at http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr0800/, or in the NRC's Agencywide Documents Access and Management System (ADAMS), at http://www.nrc.gov/reading-rm/adams.html, under Accession No. ML19256B502.

Power Plants: LWR Edition," (SRP), Section 7.1-T, "Regulatory Requirements, Acceptance Criteria, and Guidelines for Instrumentation and Control Systems Important to Safety" (Table 7-1). References to industry standards incorporated by reference into regulation (Institute of Electrical and Electronics Engineers (IEEE) Standard (Std) 279-1968, IEEE Std 279-1971, and IEEE Std 603-1991) and industry standards that are not endorsed by the agency do include the associated year in this BTP. See Table 7-1 to ensure that the appropriate RGs and endorsed industry standards are used for the review.

A. BACKGROUND

Common-cause failures (CCFs) have been identified as a type of hazard that digital I&C (DI&C) systems could be more susceptible to due to the integration capabilities provided by the technology and its inherent complexity compared to analog technologies. DI&C systems or components can also be vulnerable to a CCF due to defects in hardware, or to latent defects in the software or software-based logic. However, this BTP is focused on potential CCFs due to latent defects in the software. A CCF in a DI&C system can result in loss of a safety function through (1) systematic faults within redundant portions (e.g., safety divisions) of a safety-related system, (2) propagation of faults between safety divisions or from systems that are not safety-related (NSR) to safety-related systems, or (3) internal or external plant hazards (e.g., electro-magnetic interference). The latter two sources of CCF are primarily addressed through (1) maintaining independence between safety divisions and between safety-related systems and systems that are NSR, and (2) qualifying DI&C equipment to meet regulatory requirements, respectively. Independence encompasses physical independence, electrical independence, communications independence, and functional independence. Systematic faults are latent defects in hardware, software, or system components that can be triggered by an event or condition. A CCF of a DI&C system or component can result in loss of a safety function during a design-basis event (DBE). A CCF of a DI&C system or component can also actuate a safety-related function or other design functions without a valid demand or can result in erroneous system actions. These conditions are typically referred to as spurious operations, but the term can be used interchangeably with the term "spurious actuation." For this BTP, the term "spurious operations" is used.

In NUREG-0493, "A Defense-in-Depth and Diversity Assessment of the RESAR-414 Integrated Protection System," issued March 1979, the U.S. Nuclear Regulatory Commission (NRC) staff documented a defense-in-depth and diversity (D3) assessment of a digital computer-based reactor protection system (RPS) in which defense against software CCF (CCF hereafter), which resulted in loss of a safety function during a DBE, was based upon an approach using a specified degree of system separation between echelons of defense. The RESAR RPS consisted of the reactor trip system (RTS) and the engineered safety features (ESF) actuation system. Subsequently, in SECY-91-292, "Digital Computer Systems for Advanced Light-Water Reactors," dated September 16, 1991, the NRC staff included discussion of its concerns about CCF in digital systems used in nuclear power plants (NPPs).

As a result of reviews of applications for certification of evolutionary and advanced light-water reactor designs using DI&C systems, the NRC staff documented its position regarding vulnerabilities to CCF in DI&C systems and D3 in Item II.Q of SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR)

Designs," dated April 2, 1993. The Commission subsequently modified this position in Item 18 of the associated staff requirements memorandum (SRM) on SECY-93-087, dated July 21, 1993, in which the Commission indicated that a CCF of a DI&C system is considered a beyond-design-basis event (BDBE).

The NRC staff provided plans to the Commission to clarify the guidance associated with addressing potential CCFs of DI&C systems in SECY-18-0090, "Plan for Addressing Potential Common Cause Failure in Digital Instrumentation and Controls," dated September 12, 2018. This SECY paper documented the NRC staff's evaluation of the SRM on SECY-93-087. The staff concluded that the SRM provides adequate flexibility for regulatory modernization activities that support near-term DI&C implementation. SECY-18-0090 outlines five guiding principles to ensure consistent application of the direction provided in the SRM on SECY-93-087. These principles provide a framework for addressing potential CCFs in DI&C systems using a graded approach based on the safety significance of the DI&C system. In SECY-18-0090, the NRC staff committed to incorporating these guiding principles into the NRC staff's review guidance. In summary, while the NRC considers CCFs due to software in DI&C systems to be beyond design basis, the application should include an evaluation of potential CCFs due to software in DI&C systems and should verify that the plant is protected from the effects of these potential CCFs. In addition, the application should include an evaluation of sources of this CCF that can result in spurious operations, some of which may be considered within the design basis, as discussed later in this BTP.

Over the years, the NRC staff has approved applications with numerous design solutions, and in some cases, multiple design solutions for a single DI&C system, to address potential CCFs in DI&C systems. During these reviews, the NRC staff has observed that different solutions may be used to address potential CCFs, and that one standard solution may not be applicable to all DI&C systems. This BTP provides guidance for reviewing the applicant's or licensee's design and analysis for addressing potential CCFs due to latent software defects in I&C systems.

1. Regulatory Basis

The regulations listed below may not necessarily apply to all licensees or applicants. The applicability of these requirements is determined by the plant licensing basis and any changes to the licensing basis in the proposed DI&C system under evaluation:

- For applications of construction permits (CPs), operating licenses (OLs), combined licenses (COLs), standard design approvals (SDAs), design certifications (DCs), filed after May 13, 1999, Title 10 of the *Code of Federal Regulations* (10 CFR) 50.55a(h), "Protection and Safety Systems," requires compliance with IEEE Std 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," and the correction sheet dated January 30, 1995.

- For NPPs with CPs issued between January 1, 1971, and May 13, 1999, 10 CFR 50.55a(h), requires compliance with the requirements stated in IEEE Std 279-1968, "Proposed IEEE Criteria for Nuclear Power Plant Protection Systems," or the requirements in IEEE Std 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations," or IEEE Std 603-1991 and the correction sheet dated

January 30, 1995.

- For NPPs with CPs issued before January 1, 1971, 10 CFR 50.55a(h), requires compliance with their plant-specific licensing basis or IEEE Std 603-1991 and the correction sheet dated January 30, 1995.

- IEEE Std 603-1991, Clause 5.6.3, requires in part that "safety system design shall be such that credible failures in and consequential actions by other systems, as documented in 4.8 of the design basis, shall not prevent the safety systems from meeting the requirements of this standard." IEEE Std 603-1991, Clause 4.8, requires in part that the safety-related system design bases shall document "[t]he conditions having the potential for functional degradation of safety system performance and for which provisions shall be incorporated to retain the capability for performing the safety functions (for example, missiles, pipe breaks, fires, loss of ventilation, spurious operation of fire suppression systems, operator error, failure in non-safety-related systems)." These two clauses provide the basis for requiring plants licensed under IEEE Std 603-1991 to address the potential for spurious operation of safety-related components and components that are NSR.

- GDC 22, "Protection System Independence," requires in part "that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function. Design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protection function." GDC 22 provides the regulatory basis for requiring licensees and applicants to address the potential for CCF and for requiring the use design techniques, such as functional diversity or diversity in component design to prevent the loss of the protection function.

- 10 CFR Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants," governs applications for early site permits, DCs, COLs, SDAs, and manufacturing licenses (MLs) for nuclear power facilities.

- 10 CFR Part 100, "Reactor Site Criteria," provides guideline values for fission product releases from NPPs licensed to operate prior to January 10, 1997 that have voluntarily implemented an alternative source term under the provisions of 10 CFR 50.67, "Accident Source Term." These guideline values can be commonly referred to as the site dose guideline values and provide the acceptance criteria for radiological release limits to bound the consequences of a potential CCF concurrent with a DBE.

- 10 CFR 50.67 provides guideline values for fission product releases from currently operating NPPs that have implemented an alternative source term.

- 10 CFR 50.34(a)(1)(ii)(D) provides site dose guideline values for CP applicants and NPPs licensed to operate under 10 CFR Part 50 after January 10, 1997.

- 10 CFR 52.47(a)(2)(iv) provides site dose guideline values for standard DCs.

- 10 CFR 52.79(a)(1)(vi) provides site dose guideline values for COLs.
- 10 CFR 52.137(a)(2)(iv) provides side dose guideline values for SDAs.
- 10 CFR 52.157(d) provides site dose guideline values for ML approvals.

2. Relevant Guidance

- NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems," issued December 1994, summarizes several D3 analyses performed after 1990 and presents a method for performing such analyses. Within NUREG/CR-6303, an analysis method is presented that postulates common-mode failures that could occur within digital RPSs and determines what portions of a design need to implement additional D3 measures to address such failures. It should be noted that while these documents use the term "common-mode failure," the term "common-cause failure" is used in this BTP since it better characterizes this type of failure.
- NUREG/CR-7007, "Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems," issued December 2008, provides guidance and strategies after a D3 assessment has been performed and it is determined that diversity in a given safety-related system is needed for mitigating potential CCF vulnerabilities. NUREG/CR-7007 identifies and develops a baseline set of diversity criteria that may constitute appropriate mitigating diversity strategies to address potential CCF vulnerabilities. While this NUREG describes a method for quantitatively assessing the amount of diversity in a system, this method has not been benchmarked and should not be used as the sole basis for justifying adequate diversity.
- SECY-93-087, Item II.Q, as clarified by the SRM on SECY-93-087, Item 18, describes the NRC position concerning mitigation of potential common mode failures. It should be noted that while these documents use the term "common-mode failure," the term "common-cause failure" is used in this BTP since it better characterizes this type of failure.
- SECY-18-0090 provides the NRC staff's plan to clarify the guidance associated with evaluating and addressing potential CCFs of DI&C systems.
- Generic Letter 85-06, "Quality Assurance Guidance for ATWS Equipment That Is Not Safety-Related," dated April 16, 1985, provides quality assurance guidance for anticipated transient without scram (ATWS) equipment that is NSR. The guidance within this generic letter may be used to demonstrate the quality of equipment that is NSR and credited for providing the diverse means to mitigate a CCF.
- Regulatory Issue Summary (RIS) 2002-22, Supplement 1, "Clarification on Endorsement of Nuclear Energy Institute Guidance in Designing Digital Upgrades in Instrumentation and Control Systems," dated May 31, 2018, clarifies guidance for preparing and

documenting “qualitative assessments” that can be used to evaluate the likelihood of failure of a proposed DI&C system or component modification.

- NUREG-0800, SRP Section 7.7, “Control Systems” provides review guidance for addressing the potential for inadvertent (i.e. spurious) operation signals from control systems.

- NUREG-0800, SRP Section 7.8, “Diverse Instrumentation and Control Systems,” describes the review process and additional acceptance criteria for diverse I&C systems provided to protect against CCF.

- NUREG-0800, SRP Chapter 18, “Human Factors Engineering,” defines a methodology, applicable to both existing and new reactors, for evaluating manual operator actions as a diverse means of coping with anticipated operational occurrences (AOOs) and postulated accidents that are concurrent with a software CCF that disables a safety function credited in the safety analysis.

3. Scope

The guidance of this BTP is intended for reviews of (1) proposed modifications that require a license amendment to be implemented, and (2) applications for CPs, OLs, COLs, DCs, SDAs, and MLs. This BTP is not applicable for proposed modifications performed under the 10 CFR 50.59, “Changes, Tests and Experiments,” change process.

4. Purpose

The purpose of this BTP is to provide guidance for reviewing a licensee’s or applicant’s evaluation of (1) a DI&C system’s vulnerability to CCF due to latent defects in the software or software-based logic, (2) the diverse means credited to address remaining CCF vulnerabilities, and (3) the effects of any unmitigated CCF vulnerabilities on plant safety. This BTP also provides guidance on implementing a graded approach to address the potential for CCF due to latent defects in the software or software-based logic in DI&C systems based on the safety-significance of the system. In this guidance, software includes software, firmware[1] and logic developed from software-based development systems (e.g., hardware description language programmed devices).

This BTP is intended to address CCFs caused by a software design defect, which is considered a BDBE for structures, systems, and components (SSCs) that employ a robust design process to reduce the likelihood of design defects. The plant response to these BDBEs may be analyzed using either conservative or best-estimate methods. However, in integrated DI&C systems, a single random hardware failure can have cascading effects, similar to a CCF (e.g., loss of multiple functions within a safety group, or spurious operation of functions within multiple safety groups). Single random hardware failures with cascading effects are considered DBEs, because random hardware failures are expected during the life of the facility. DBEs should be

[1] IEEE 100, “The Authoritative Dictionary of IEEE Standards Terms,” defines firmware as the combination of a hardware device and computer instructions and data that reside as read-only software on that device.

analyzed using conservative methods to demonstrate that the plant response to these events are bounded by the events in the safety analysis. RG 1.53 provides guidance for the deterministic analysis of single failures in safety-related systems.

This BTP provides guidance for reviewing (1) design measures, such as the use of diverse equipment within a system or component to prevent CCF, (2) diverse external equipment, including manual controls and displays to mitigate a CCF, and (3) other defensive measures to ensure conformance with the NRC's position on addressing potential CCFs in DI&C systems as specified in the SRM on SECY-93-087 and SECY-18-0090. The objectives of this review are to verify the following:

- Vulnerabilities to CCF have been adequately identified and addressed for DI&C systems using a graded approach based on the safety significance of the system.

- For DI&C systems of high safety significance, an adequate D3 assessment has been performed to meet the acceptance criteria described in this BTP. This D3 assessment should consist of (1) an evaluation of vulnerabilities to CCF due to latent design or implementation defects within this system, (2) the identification of credited diverse means to address CCFs that have not been eliminated from further consideration, and (3) the performance of an assessment of the consequences of residual CCFs that have not been mitigated to demonstrate that the consequences remain bounded by the events analyzed in the safety analysis. The term "bounded" as used in this BTP means that the plant conditions remain within the acceptance criteria of the events analyzed in the safety analysis.

- A qualitative assessment has been performed for proposed DI&C systems of lower safety significance, and the results of this assessment meet the acceptance criteria within this BTP.

- If defensive measures or design attributes are used in a proposed DI&C system to eliminate the CCF from further consideration, these defensive measures or design attributes are adequate.

- If diversity has been provided in a design to prevent or mitigate a CCF, the diversity measures are adequate.

- If manual means for performing the safety function(s) are credited to mitigate a potential CCF of the DI&C system, the operator has access to diverse displays and manual controls that are not subject to the same CCF and the time margin for crediting manual operation meets the criteria for manual controls established by the guidance within SRP Chapter 18.

This BTP also addresses CCFs due to latent software defects that can cause the spurious operation of a safety-related components or components that are NSR because such spurious operations have the potential to put the plant in a condition that has not been previously analyzed in the safety analysis. If these conditions have not been analyzed, then such conditions may not be adequately mitigated by an I&C system. This BTP provides criteria for assessing potential spurious operation of safety-related components or components that are

NSR due to a postulated CCF of a DI&C system or component.

B. BRANCH TECHNICAL POSITION

1. Introduction

1.1. Four Common-Cause Failure Positions and Clarification

The foundation of BTP 7-19 is the "NRC position on D3" from the SRM on SECY-93-087, Item 18. The four positions stated in the SRM on SECY-93-087 are quoted below:

Position 1 "The applicant shall assess the defense-in-depth and diversity of the proposed instrumentation and control system to demonstrate that vulnerabilities to common -mode failures have adequately been addressed."

Position 2 "In performing the assessment, the vendor or applicant shall analyze each postulated common-mode failure for each event that is evaluated in the accident analysis section of the safety analysis report (SAR) using best-estimate methods. The vendor or applicant shall demonstrate adequate diversity within the design for each of these events." (emphasis in original).

Position 3 "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." (emphasis in original).

Position 4 "A set of displays and controls located in the main control room shall be provided for manual, system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. The displays and controls shall be independent and diverse from the safety computer system identified in Items 1 and 3 above."

SECY-18-0090 clarifies the application of the Commission's direction in the above four positions to reduce regulatory uncertainty. In accordance with Position 1 of SRM on SECY-93-087, Item 18, a D3 assessment should be performed. Section B.3 of this BTP provides review guidance and acceptance criteria for this assessment to demonstrate that vulnerabilities to CCFs have been adequately addressed. The guiding principles within SECY-18-0090 clarify that the applicant or licensee could use a graded approach to determine the degree of rigor that is necessary to accomplish the D3 assessment. This graded approach is described in Section B.2.1 of this BTP.

The term "best estimate methods" in Position 2 is now referred to as methods using "realistic assumptions," which are defined as the initial plant conditions corresponding to the onset of the

event being analyzed. Initial plant event conditions include the following:

- power levels
- temperatures
- pressures
- flows
- alignment of equipment
- availability of plant equipment not affected by the postulated CCF

The guiding principles within SECY-18-0090 clarify that in addition to "best estimate methods" identified in Position 2 of SRM on SECY-93-087, Item 18, the D3 assessment can be performed using a design-basis analysis (i.e., conservative methods). Thus, when performing the D3 assessment, the applicant or licensee may use realistic assumptions to analyze the plant response to DBEs, or the conservative assumptions on which the safety analysis is based. This safety analysis is normally documented in Chapter 15 of the Final SAR (FSAR) or Updated FSAR (UFSAR), but it could be in other chapters. Hereafter, the term "safety analysis" will be used without specifying whether this analysis is documented in the FSAR or UFSAR. Each event analyzed within the safety analysis should be evaluated in the D3 assessment independently. For example, if the initiating event is the loss of offsite power, the assessment does not need to assume another concurrent DBE.

If the D3 assessment indicates a postulated CCF could disable a safety function, then Position 3 directs that an applicant or licensee should identify an existing diverse means or add a diverse means to perform the safety function or a different function. The diverse means may be equipment that is NSR with a documented basis that the diverse means is of sufficient quality and unlikely to be subject to the same CCF. While the enclosure to Generic Letter 85-06 provides quality assurance guidance for ATWS equipment, this guidance can also be applied to equipment that is NSR credited as the diverse means for addressing potential CCFs. SECY-18-0090 clarifies that use of either automatic or manual actuation within an acceptable time frame is an acceptable means of diverse actuation. SECY-18-0090 also specifies that if the D3 assessment demonstrates that a postulated CCF can be reasonably mitigated through other means such as with current systems, an added diverse means that performs the same or a different function may not be needed. For example, an ATWS system may be credited as the diverse means, provided it is not subject to the same CCF that disabled the safety function.

If a diverse means is part of a safety division, it would then be subject to meeting divisional independence requirements in IEEE Std 603-1991, Clause 5.6.1, which is incorporated by reference pursuant to 10 CFR 50.55a, "Codes and Standards." If the diverse means is NSR, then the IEEE Std 603-1991, Clause 5.6.3 requirements for separation and independence between safety-related systems and systems that are NSR should be met.

Position 4 directs the inclusion of a set of displays and manual controls (safety or nonsafety) in the main control room (MCR) that is diverse from any CCF vulnerability identified within the "safety computer system" discussed in Positions 1 and 3 above and meets divisional independence requirements as applicable for the specific design implementation. While the SRM on SECY-93-087 uses the terms "safety" and "nonsafety," the NRC staff interprets this as safety-related and NSR, respectively. These displays and controls should provide manual

system or divisional level, depending on the design, actuation and control of equipment to manage the “critical safety functions” (see Section B.1.2). Further, if not subject to the same CCF as the proposed safety-related DI&C system, some of these displays and manual controls from Position 4 may be credited as all or part of the diverse means provided to address Position 3. SECY-18-0090 did not provide any clarification for Position 4.

The Position 4 phrase “safety computer system identified in Items 1 and 3 above” refers to the safety-related DI&C system that is credited for mitigating the AOO and postulated accident in the safety analysis. Typically, the automatic safety-related I&C system is credited, but for some events, manual safety-related controls are the ones credited.

The four positions from the SRM on SECY-93-087, Item 18, are based on the NRC concern that DI&C system development errors are a credible source of CCF. Generally, DI&C systems containing software or logic cannot be fully tested except for very limited cases, nor can their failure modes be completely predicted because software does not have a physical manifestation that limits its behavior. Therefore, the NRC staff considers DI&C systems vulnerable to CCF because either (1) identical system designs and identical copies of the software or software-based logic are present in redundant divisions of safety-related systems or (2) previously separated functions have been integrated into a single DI&C system. Also, some errors, such as those labeled as “software design errors,” normally result from errors in the higher-level requirements (e.g., system requirements or design specifications), in which the system design misrepresents the actual process. As used in this BTP, the term “higher-level requirements” and the like do not refer to NRC regulatory requirements but to system or component design or operating characteristics upon which the applicant or licensee relies to accomplish the stated system or component functions. Throughout this BTP, context will indicate whether requirements are NRC regulatory requirements or “higher-level requirements.”

SECY-18-0090 recognizes that although significant effort has been applied to the development of highly reliable DI&C systems, the NRC staff believes that some residual faults may remain undetected within a system and could result in hazards that can challenge plant safety. This includes hazards that result from loss of the safety function or those caused by spurious operation of a safety function or other design function. To address these potential hazards, the NRC staff should verify that the application has (1) identified potential hazards due to a design or implementation defect in a DI&C system and associated impacts to the intended safety function or other design functions, (2) demonstrated that a CCF due to these residual defects has been either adequately prevented through use of appropriate measures (e.g., diversity within the design, testing, and defensive measures) or mitigated through use of a diverse means, and (3) assessed the ability of the overall plant design (e.g., I&C systems, mechanical systems, and manual operator actions) to maintain plant safety, using conservative or “best estimate” methods, for those CCFs that have not been shown to be prevented or mitigated.

1.2. Critical Safety Functions

In the revised SECY-93-087, Item II.Q, included with the SRM, the NRC staff identified the following critical safety functions to be managed from the MCR per Position 4 of this SRM: :

- reactivity control
- core heat removal

- reactor coolant inventory
- containment isolation
- containment integrity

Therefore, a safety function identified in the safety analysis may not always be a “critical safety function,” as defined in the SRM on SECY-93-087.

2. Graded Approach and Level of Integration for Addressing Common-Cause Failure

2.1. Graded Approach for Categorizing Digital Instrumentation and Control Systems

For assessing vulnerabilities to CCF, a graded approach refers to analyses performed for equipment of differing safety significance in which CCF concerns apply. For example, a CCF analysis for a digital RTS would be expected to be more rigorous than a CCF analysis for a safety-related MCR Heating, Venting, and Air Conditioning (HVAC) chiller. While the HVAC chiller is a safety-related system that maintains certain temperature and humidity in the MCR for equipment and personnel to operate properly, a failure of this system is not as significant as the failure of the RTS because operators will have operating procedures or diverse means to control temperature and humidity and will shutdown the plant, if necessary. Table 2-1 depicts a categorization scheme for implementation of this graded approach that is based on the classification of the DI&C system and its safety significance.

Table 2-1: Categorization Scheme for Implementing a Graded Approach To Address CCF

	Safety-Related	NSR
Safety Significant— Significant contributor to plant safety	**A1**	**B1**
Not Safety Significant— Not a significant contributor to plant safety	**A2**	**B2**

The following criteria should be used to determine the category of a DI&C system:

a. A1: DI&C system that is safety-related—

   1. that is relied upon to initiate and complete control actions essential to maintain plant parameters within acceptable limits established for a DBE; or

   2. whose failure could directly lead to accident conditions that may cause unacceptable consequences (i.e., exceeds acceptable limits for a DBE) if not mitigated by other A1 systems.

b. A2: DI&C system that is safety-related—

1. provides an auxiliary or indirect function in the achievement or maintenance of plant safety; or

2. maintains the plant in a safe shutdown state after the plant has reached initial safe shutdown state[2].

c. B1: DI&C system that is NSR—

1. that directly changes the reactivity or power level of the reactor, or affects the integrity of the safety barriers (fuel cladding, reactor vessel, or containment); or

2. whose failure may result in unacceptable consequences to plant safety due to integration of multiple control functions into a single system.

d. B2: DI&C system that is NSR—

1. that does not have a direct effect on reactivity or power level of the reactor; and

2. whose failure does not have consequences to plant safety or whose failure can be detected and mitigated with significant safety margin.

Risk insights in terms of safety consequences from site-specific probabilistic risk assessments (PRAs) can be used to support the safety-significance determination in categorizing the DI&C system. Use of such risk insights should be an input to an integrated decision-making process for categorizing the proposed DI&C system. The application should document the basis for categorizing the proposed DI&C system, including any use of risk insights.

The application should address the following criteria regarding the potential for CCFs in the proposed system:

a. For an A1 system, the application should include a D3 assessment in accordance with the criteria in Section B.3.

b. For an A2 or B1 system, the application should include a qualitative assessment in accordance with Section B.4 to address potential CCFs.

c. For a B2 system, the application should include a qualitative assessment if the proposed design could introduce conditions that have not been previously analyzed in the safety analysis due to the proposed implementation of combined design functions, shared resources, or connectivity to other plant systems. The basis for not performing a qualitative assessment should be documented.

These criteria are consistent with SECY-18-0090, which states that “an analysis may not be necessary for some low-safety-significance I&C systems whose failure would not adversely affect a safety function or place a plant in a condition that cannot be reasonably mitigated.” In accordance with the criteria within Section B.3, the process flow for performing a D3 assessment to address potential CCFs in an A1 system is depicted in Figure 2-1. The process flow for performing a qualitative assessment to address potential CCFs in an A2 or B1 systems is depicted in Figure 2-2.

[2] The plant safe shutdown state is site-specific, as defined in the site’s licensing and design bases.

System integration and interconnectivity among the categories identified in Table 2-1 can introduce additional vulnerabilities to CCF. If there is integration (e.g., through combined design functions, shared resources, or digital interconnectivity) among A1 systems or among A1 and systems in the other three categories, then the assessment for the proposed A1 system should consider the susceptibility to CCF of the integrated system and the consequences of CCFs that could affect the integrated or interconnected A1 systems. For example, if a digital protection system includes controllers for performing reactor trip and ESF logic as well as safety-related control functions (e.g., auxiliary feedwater level control), and the reactor trip or ESF initiation signal only reaches the final actuation device via the equipment that perform these safety-related control functions, then the categorization of all the equipment in that pathway should be A1. A D3 assessment should be performed in accordance with the guidance in Section B.3 on these interconnected or integrated systems. In performing this assessment, the criteria in Section B.3.1 for an A1 system apply to these interconnected or integrated systems.

2.2. Common-Cause Failure Assessment Commensurate with Level of Integration and Interconnectivity

If the licensee or applicant can demonstrate that existing or newly created interfaces or interconnections between A1 systems and systems in other categories do not have the potential to adversely impact the operation of the A1 systems (e.g., use of one-way digital communications output from the A1 system to systems in other categories rather than bi-directional communications) or reduce defense-in-depth, then the impacts of failures occurring within the non-A1 system(s) can be excluded from the D3 assessment for the A1 system. However, it is still necessary to ensure that CCFs occurring within or among the systems in the other categories do not result in plant conditions that have not been previously analyzed in the safety analysis. Section B.4 contains criteria on performing a qualitative assessment.

3. Diversity and Defense-in-Depth (D3) Assessment

To defend against potential CCF, the NRC staff considers the performance of a D3 assessment using a three-step process to be key in the implementation of A1 systems: (1) determining whether CCF vulnerabilities exist in the proposed A1 system that have not been eliminated from further consideration using design attributes, defensive measure, or testing; (2) demonstrating that diverse means provided to perform the same or a different function are sufficient for those CCFs that have not been eliminated from further consideration; and (3) demonstrating that consequences due to remaining CCF vulnerabilities are bounded. The application should include the results of a D3 assessment that conforms to the following:

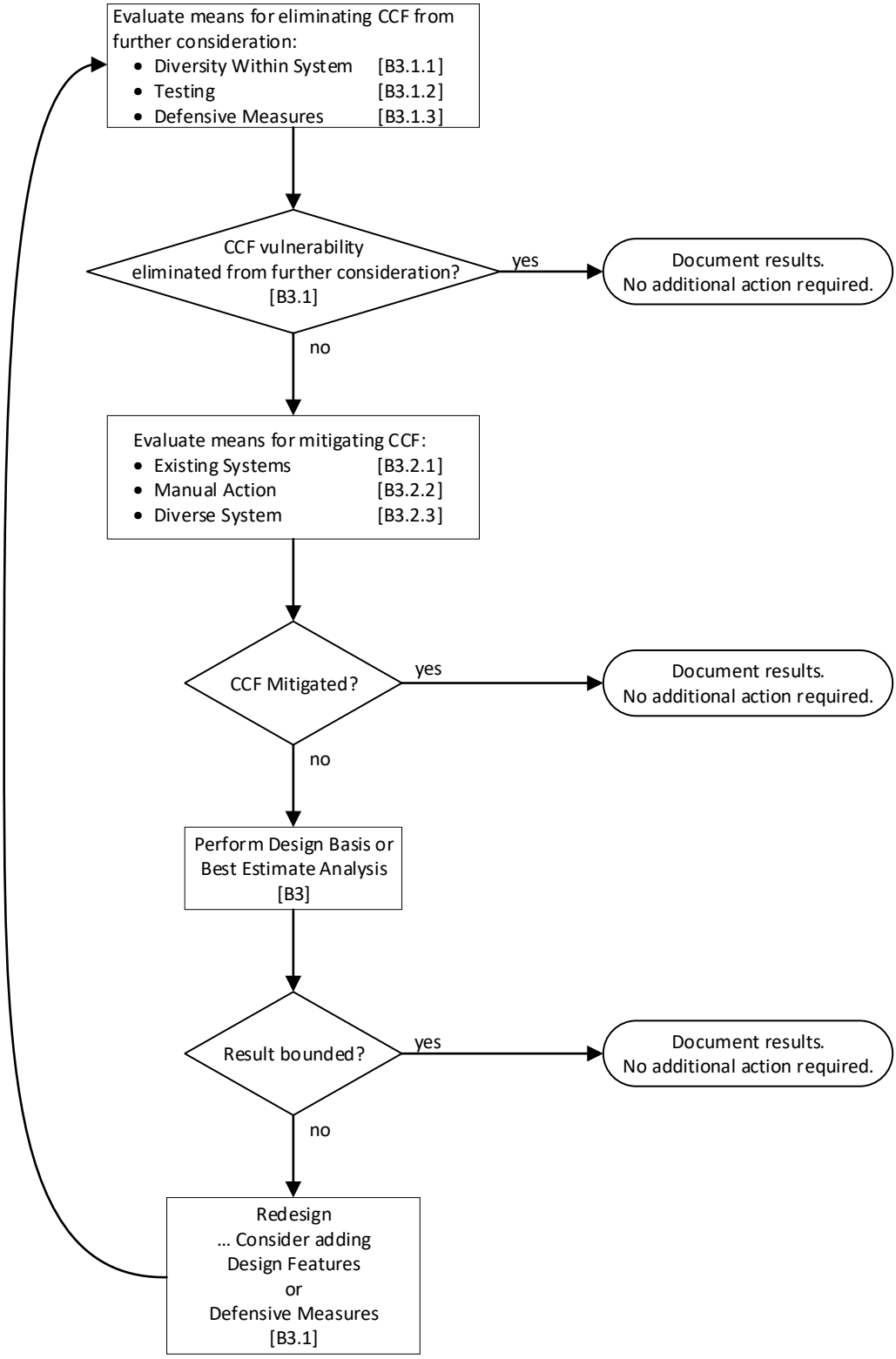

Figure 2-1: D3 Assessment Process Flow for an A1 System

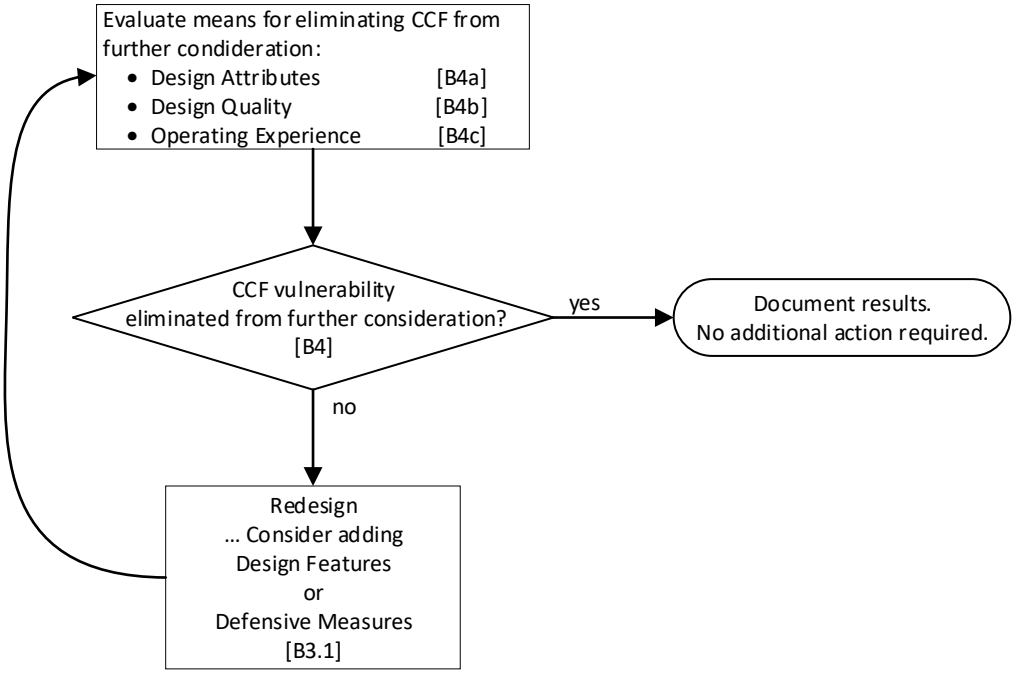

Figure 2-2: Qualitative Assessment Process Flow for an A2 or B1 System

a. In accordance with Position 1 of the SRM on SECY-93-087, Item 18, the application should include the results of a D3 assessment. The D3 assessment should determine whether an A1 system is vulnerable to a CCF. Acceptable means that can be used to conclude an A1 system is not vulnerable to a CCF are provided in Section B.3.1. If the means identified in Section B.3.1 are credited to eliminate CCF from further consideration for an A1 (or portions of an A1) system, then the D3 assessment will only need to identify and document the credited means and demonstrate the effectiveness of these means. In this case, items b. and c. below (i.e., Positions 2 and 3 of the SRM on SECY-93-087, Item 18, respectively) of this subsection would not apply to the A1 system or to portions of the A1 system under consideration.

b. In accordance with Position 2 of the SRM on SECY-93-087, Item 18, and the clarifications in SECY-18-0090, either best estimate methods (i.e., using realistic assumptions to analyze the plant response to DBEs) or conservative methods (i.e., design-basis analysis) may be used to perform the D3 assessment.

c. In accordance with Position 3 of the SRM on SECY-93-087, Item 18, 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 a documented basis should be provided in the application. The D3 assessment should identify the safety functions that are vulnerable to CCF and either (1) identify and document the diverse means that are credited for performing the same function or a different function, or (2) demonstrate that the consequences are within acceptable limits for each AOO or

postulated accident within the safety analysis. Section B.3.2 provides criteria for acceptable diverse means.

A D3 assessment may credit one or more of the acceptable means identified in Sections B.3.1 and B.3.2 to address vulnerabilities to CCF. This includes crediting appropriate design features that prevent the occurrence of CCFs as well as crediting appropriate design measures that limit or mitigate the effects of potential CCFs.

When the RTS or ATWS mitigation system in an operating plant is modified, the requirements of the ATWS rule as specified in 10 CFR 50.62, "Requirements for Reduction of Risk From Anticipated Transients Without Scram (ATWS) Events for Light-Water-Cooled Nuclear Power Plants," must be met. In 10 CFR 50.62, the NRC requires that the ATWS mitigation system be composed of equipment that is diverse from the RTS.

Acceptance Criteria

The D3 assessment included in the application should demonstrate compliance with the NRC position on D3 described above. To reach a conclusion of acceptability, the following criteria should be met and supported by summation of the results of the assessment.

a. If any means as described in Section B.3.1 are credited to eliminate the CCF from further consideration for the A1 or portions of the A1 system, the application has met the acceptance criteria for these credited means. In this case, items b. through d. of this subsection would not be applicable to the A1 or portions of the A1 system.

b. If an A1 system is vulnerable to a CCF, then any of the diverse means provided in Section B.3.2 can be used to address the CCF. If a diverse means is provided to perform the same or a different function as the A1 system affected by the CCF, then items c. and d. below are not applicable. The application should show that these diverse means are—

    1. capable of responding with sufficient time available for the operators to determine the need for safety actions even with indicators that may be malfunctioning due to the CCF, if manual operator actions are credited in the D3 assessment

    2. capable of effectively performing the same or a different function in response to the DBE

    3. supported by sufficiently independent instrumentation that indicates—

        i. whether the safety function is needed

        ii. whether the A1 system did not perform the safety function

        iii. whether the automated diverse means or manual action is successful in performing the safety function

c. For each AOO in the design basis occurring in conjunction with each single postulated CCF, the plant response calculated using realistic or conservative assumptions does not result in radiation release exceeding 10 percent of the applicable siting dose guideline values or violation of the integrity of the primary coolant pressure boundary.

d. For each postulated accident in the design basis occurring in conjunction with each single postulated CCF, the plant response calculated using realistic or conservative assumptions does not result in radiation release exceeding the applicable siting dose guideline values, violation of the integrity of the primary coolant pressure boundary, or violation of the integrity of the containment (i.e., exceeding coolant system or containment design limits).

The adequacy of the diversity provided with respect to the above criteria should be justified in the application and explicitly addressed in the NRC staff's safety evaluation.

3.1. Means to Eliminate Further Consideration of Common-Cause Failure

Many system design and testing attributes, procedures, measures, and practices can contribute to significantly reducing the likelihood of CCF. However, there are certain design attributes that are sufficient to eliminate further consideration of a CCF due to a digital design or implementation defect. These attributes include diversity within the DI&C system or component and testability. If the application demonstrates that these design attributes of proposed DI&C systems or components meet the criteria within this BTP, then separate diverse means do not need to be provided, and an analysis of the plant's response for each AOO or postulated accident concurrent with the postulated CCF of the A1 system does not need to be performed for those proposed systems or components. Criteria for demonstrating that each of these design attributes is sufficient are provided in Sections B.3.1.1 and B.3.1.2.

In addition to the two attributes discussed in the preceding paragraph, appropriate defensive measures can be used in the design of proposed A1 systems and components to prevent CCFs from occurring, or to limit or mitigate the consequences of CCFs. If the application demonstrates that these defensive measures meet the criteria within this BTP, then separate diverse means do not need to be provided and a coping analysis does not need to be performed for those proposed systems or components. Criteria for demonstrating that design measures are sufficient are provided in Section B.3.1.3 of this document.

3.1.1. Use of Diversity Within the Digital Instrumentation and Control System or Component To Eliminate Further Consideration of Common-Cause Failure

If sufficient diversity exists within each safety division or among redundant safety divisions of an A1 system to perform the safety function, then the potential for CCF can be considered to be appropriately addressed without further action. For example, a digital protection system could be designed such that each credited safety function is implemented in one division that uses one type of digital technology and another division that uses a different digital technology. In this case, the application should include an analysis to demonstrate that sufficient diversity exists between these two divisions of the digital protection system such that they are not subject to the same CCF. If this can be demonstrated, the CCF vulnerability can be considered

eliminated from further consideration.

It should be noted that since each redundant safety-related division is credited for compliance with the single-failure criterion and is now additionally credited to prevent CCF, the allowable time that a division can be bypassed as specified in the technical specification may be more restrictive than if the redundancy is solely credited for meeting the single-failure criterion. This is specific for each application.

Acceptance Criteria

To reach a conclusion that sufficient diversity exists within the A1 system, the following criteria should be met:

a. Each safety function to be achieved by the proposed design is shown to be independently achievable by each different design used in the system.

b. The diverse portions of the system or component do not have common or shared resources, such as power supplies, memory, bus, or communications modules that could affect both diverse designs, nor do the diverse designs share engineering or maintenance tools, which could become a source of common-cause vulnerability.

c. Each diverse design used to perform the credited safety functions is shown to be highly reliable and continually available for the plant conditions during which the associated event is expected to be prevented or mitigated.

d. Periodic surveillance criteria are used to verify the continued operability of each diverse design.

3.1.2. Use of Testing to Eliminate Further Consideration of Common-Cause Failure

When considering potential sources for CCF in DI&C systems or components, there are two general areas of concern: (1) CCF as a result of errors introduced by the system or software requirements, and (2) CCF as a result of errors introduced during the design and implementation of the software or software-based logic. A quality design process can be credited to address potential errors in the system or component design requirements or specifications; this is the case for both analog and digital equipment. However, this does not address potential defects introduced during the design and development process. Testing may be credited as a means to identify and address potential CCFs in a digital device or component as a result of potential latent defects in the design, fabrication, and implementation of software or software-based logic.

The set of test cases applicable to systems with a large number of inputs or with even a small amount of memory can become impracticably large. The testing approach provided below is intended for application to devices and components that are simple enough for such testing to be practical. To credit testing as a means of demonstrating potential design, fabrication, and implementation errors have been identified and corrected such that the device and component will function as specified under the anticipated operational conditions, the application should demonstrate the following test methods are included:

a. The combination of every possible input is included in the testing. Any unused input that are permanently forced to a fixed state can be at that fixed state during this testing. For analog inputs, the verification of proper calibration can be accomplished separately. For this functional testing, each analog signal needs only be tested at values known to be above and below the associated setpoints.

b. Where the output of a device or component depends upon timing of the input or timing of internal state changes, then the testing should include all possible timing sequences in the testing.

c. If the device or component includes any kind of memory, such that the response to the current set of inputs is dependent upon some past condition, then all possible past condition sequences should be included in the testing or shown through analysis to not impact the device output.

d. If a device or component includes logic or circuits that are not used under any operational condition, and it is demonstrated that the unused logic or circuitry cannot interfere with the proper operation of the device regardless of (1) any possible malfunction or failure within the device, (2) any condition external to the device, or (3) any aspect of the operation of any other logic or circuits included in the device, then these unused logic or circuitry can be excluded from the test cases.

Other testing methods may be acceptable and should be reviewed on a case-by-case basis. The application should provide the technical basis for using other testing methods and for how these methods are acceptable.

Acceptance Criteria

To reach a conclusion that sufficient testing has been performed on a device or component such that CCF can be eliminated from further consideration, the following criteria should be met:

a. All possible combinations of inputs have been tested as described above and the outputs have been verified to show that the output is correct for each set of inputs.

b. If the device or component depends on the timing of inputs or the timing of internal state changes, all possible timing sequences have been tested and the outputs have been verified to show that the output is correct for each set of inputs.

c. If the device or component includes any kind of memory, such that the response to the current set of inputs depends upon some past condition, then all possible past conditions have been included in the testing or have been shown through analysis to not impact the device output.

d. If a device or component includes logic or circuits that are not used under any operational condition and is therefore exclude from the test cases, the unused logic or circuitry has been shown to not interfere with the proper operation of the device regardless of (1) any possible malfunction or failure within the device, (2) any condition

external to the device, or (3) any aspect of the operation of any other logic or circuits included in the device.

3.1.3. Use of Defensive Measures to Eliminate Further Consideration of Common-Cause Failure:

In addition to having diversity within the design or performing testing, there may be defensive measures that are effective to prevent, limit, or mitigate the effects of a potential CCF in a DI&C system. If the application credits the use of such defensive measures to eliminate potential CCFs from further consideration, the application should include the following:

a. an identification of the vulnerabilities or hazards for which the defensive measures are being applied

b. a description of the defensive measures being credited to address the identified vulnerabilities or hazards

c. a description of how the potential CCF hazard will be prevented, limited, or mitigated by the proposed design measures

d. the technical basis that describes why the selected defensive measures are acceptable to address the identified vulnerabilities such that the effects of a postulated CCF are limited, mitigated or prevented, including an analysis of how the effectiveness of the measures credited can be demonstrated

e. an assessment of any residual risks from potential CCFs

If an application (e.g. license amendment request, NRC-approved industry guidance or design certification) credits use of defensive measures to address potential CCFs in a DI&C system, the defensive measures being credited along with a supporting technical basis and acceptance criteria, should be based upon an NRC-approved methodology or described as part of the application submitted to NRC staff for approval.

Acceptance Criteria

The credited defensive measures to address CCF in a DI&C system or component along with the documented supporting technical basis and acceptance criteria, are based upon an NRC-approved methodology. If technical basis and acceptance criteria are submitted in the application, the NRC staff will review and approve on a case-by-case basis.

3.2. Use of Diverse Means to Address Common-Cause Failures

Per Position 3 of the SRM on SECY-93-087, Item 18, a diverse mean should be provided to accomplish the same or different function than the safety function disabled by the postulated CCF. Sections B.3.2.1 through B.3.2.3 provide acceptable diverse means to meet Position 3 of the SRM on SECY-93-087, Item 18.

3.2.1. Crediting Existing Systems

As a means of addressing CCF of an A1 system, an existing highly reliable I&C system can be used to perform the same safety function or a different function from the intended safety function disabled by a postulated CCF. The function performed by this existing I&C system should result in plant consequences that do not exceed the limits prescribed for each AOO or postulated accident in the safety analysis. An analysis should be performed to demonstrate that the existing plant system to be credited and the digital design used for the proposed A1 system are not subject to the same postulated CCF. Section 2.6 of NUREG/CR-6303 identifies six diversity attributes and 25 related diversity criteria that can be used to support this qualitative analysis.

The existing system may be a system that is NSR provided it is of sufficient quality and can reliably perform the required functions under the associated event conditions. For existing systems that are NSR, the quality of these systems should be similar to systems required by the ATWS rule (i.e., 10 CFR 50.62), as described in the enclosure to Generic Letter 85-06. For example, plant ATWS design capabilities may be credited as a diverse means of achieving reactor shutdown, provided that the ATWS system design to be credited is capable of responding to the same analyzed events as the proposed A1 system. The ATWS system to be credited should (1) be diverse from the proposed DI&C system; (2) has been demonstrated to be highly reliable and of sufficient quality; and (3) be responsive to the AOO or postulated accident sequences using independent sensors and actuators as the proposed DI&C system.

Acceptance Criteria

To reach a conclusion of acceptability for crediting an existing plant system as the diverse means used to perform the same or a different function as the proposed DI&C system, the following criteria should be met:

a. The equipment to be credited is highly reliable, of sufficient quality, and is expected to be available during the associated event conditions.

b. The equipment to be credited is not subject to the same postulated CCF as the proposed DI&C system.

c. The equipment to be credited (1) has the capabilities of sensing and responding to the same plant conditions as the affected system if performing the same safety function, or (2) is capable of sensing and responding to alternative plant conditions if performing a different function. For both these options, the capabilities for sensing and responding have been shown to maintain plant safety by verifying plant conditions are within the recommended acceptance criteria for each AOO or postulated accident in the safety analysis.

3.2.2. Crediting Manual Operator Actions

Manual operator actions within an acceptable time frame can be used as a diverse means to provide the same or a different function credited in the D3 assessment. If manual operator actions are used as the diverse means, the equipment necessary to perform these actions,

including the supporting indications, should be diverse and independent from the safety-related I&C system disabled by a potential CCF. If the equipment used to perform these manual operator actions are NSR, then the application should include information to demonstrate that the equipment used are highly reliable and of sufficient quality. This equipment should be similar in quality as those required by the ATWS rule (i.e., 10 CFR 50.62), as described in the enclosure to Generic Letter 85-06. Functional characteristics (e.g., range, accuracy, time response) should be sufficient to provide operators with the information needed to place and maintain a plant in a safe-shutdown condition. A CCF that affects normal displays or controls should not prevent the operator from manually performing the safety functions.

The application should contain an HFE analysis to demonstrate that plant conditions can be maintained within recommended acceptance criteria for the particular AOO or postulated accident. The credited manual operator actions and the equipment necessary to perform these actions should be identified. If equipment outside of the MCR is used to perform these actions, then the reliability, availability, and accessibility of the equipment under the postulated event conditions should be demonstrated. HFE principles and criteria should be applied to the selection and design of the displays and controls. Human-performance requirements should be described and related to the plant safety criteria. Recognized human-factors standards and design techniques should be employed to support the described human-performance requirements.

Acceptance Criteria

To reach a conclusion of acceptability of manual operator actions as the diverse means used to perform the same or a different function as the automatic DI&C system, the following criteria should be met:

a. The manual operator actions can be performed within an acceptable time frame as specified in SRP Chapter 18. The difference between time available, as determined by the thermal-hydraulic analysis, and the time required, as determined by the HFE analysis, for operator action is a measure of the safety margin. As this margin decreases, the uncertainty in the estimate of the difference between these times should be appropriately considered. This uncertainty could reduce the level of assurance and potentially invalidate a conclusion that operators can perform the action reliably within the time available. For complex situations and for actions with limited margin between time available and time required, a more focused staff review will be performed.

b. The equipment used to support manual operator action is diverse, reliable, of sufficient quality, available, and accessible during the associated event conditions.

c. The indications and controls needed to support the manual operator action has the functional characteristics necessary to maintain the plant within the accepted limits.

d. The HFE analysis demonstrates the acceptance criteria provided in SRP Chapter 18, have been met.

3.2.3. Crediting a Diverse System

A diverse system (e.g., diverse actuation system), including automated or manual functions, or both, could be credited as a diverse means to address CCF. If such a system is credited as a diverse means to address CCF, the application should demonstrate that (1) the functions performed by this diverse means are adequate to maintain plant conditions within recommended acceptance criteria for the particular DBE, and (2) sufficient diversity exists between this diverse system and the A1 system subject to the CCF. An analysis should be performed to demonstrate that the diverse means to be credited and the digital design used for the proposed A1 system are not subject to the same postulated CCF. Section 2.6 of NUREG/CR-6303 identifies six diversity attributes and 25 related diversity criteria that can be used to support this qualitative analysis.

The diverse means may be performed by a system that is NSR, if the system is of sufficient quality to perform the necessary function(s) under the associated event conditions. The diverse means should be similar in quality to systems required by the ATWS rule (i.e., 10 CFR 50.62), as described in the enclosure to Generic Letter 85-06.

Prioritization between A1 systems and the diverse system should address the following to ensure the credited safety function can be accomplished by either system:

a. Commands that direct a component to a safe state should always have the highest priority and override other commands. The term “safe state” refers to a predetermined design state of least critical consequence.

b. For those components with multiple safe states, in which each safe state is defined by the plant conditions, priority should be assigned based upon considerations relating to plant system design to minimize consequence to plant safety.

c. The basis behind the proposed priority ranking should be explained in detail.

d. The priority function should be shown to apply the commands correctly in order of their priority rankings and should meet all other applicable guidance.

Acceptance Criteria

To reach a conclusion of acceptability for use of the diverse system, the following criteria should be met:

a. The functions performed by this diverse system are adequate to maintain plant conditions within the accepted limits for the particular DBE.

b. Sufficient diversity exists between this diverse system and the A1 system subject to the CCF.

c. The equipment to be credited has the required functional characteristics necessary to maintain the plant within the accepted limits.

d. Any use of priority functions to prioritize between the diverse system and the A1 system or other systems/manual operator actions has been shown to ensure that the commands that direct a component to a safe state or to the state that minimizes consequences to plant safety for those components with multiple safe states have the highest priority, and the documented basis for the priority ranking is appropriate.

e. If equipment that is NSR is used in the diverse system, the equipment is highly reliable and of sufficient quality to perform the necessary function(s) during the associated event conditions.

4. Qualitative Assessment

RIS 2002-22, Supplement 1, describes a methodology that the NRC staff finds acceptable to assess the likelihood of failure of a proposed modification of a SSC with digital technology, referred to as a qualitative assessment. The qualitative assessment described in RIS 2002-22, Supplement 1, is intended for modifications to SSCs of low safety significance (i.e., A2 and B1) and not for SSCs of high safety-significance (i.e., A1 systems).

The qualitative assessment considers three factors that, when taken in the aggregate, can be used to demonstrate that a proposed digital modification to an SSC will exhibit a low likelihood of failure (e.g., low likelihood of CCF), consistent with the safety analysis assumptions for the proposed DI&C system. These three factors include:

a. design attributes and features of the DI&C system or component;

b. quality of the design process of the DI&C system or component; and

c. applicable operating experience regarding the DI&C system or component.

Consideration of these factors, as well as supporting failure analysis information as described in RIS 2002-22, Supplement 1, is an acceptable method to address potential CCF vulnerabilities in A2, B1, and applicable B2 systems. The application should include a qualitative assessment that documents (1) how these three factors have been used to reduce the likelihood of a CCF to eliminate it from further consideration, and (2) the supporting failure analysis.

Acceptance Criteria

As described in RIS 2002-22, Supplement 1, the acceptance criteria used to determine whether an SSC has a low likelihood of failure such that current licensing assumptions continue to be met are referred to as “sufficiently low.” The concept of sufficiently low was developed to address the likelihood of a CCF due to latent digital defects of a system or component modified with digital technology. The “sufficiently low” definition incorporates consideration of failure likelihood of a proposed SSC to failures documented in the safety analysis. This approach can also be used for a new reactor design, where by the likelihood of failure of a DI&C system or component should be aligned with the assumptions in the safety analysis.

To reach a conclusion of acceptability, the following criteria should be met and supported by summation of the results of the qualitative assessment:

a. Design attributes and features have been implemented and shown to provide reasonable assurance of effectiveness for reducing the likelihood of potential CCFs such that their occurrence is sufficiently low.

b. Quality of the design process of the DI&C system provides reasonable assurance that the potential for CCFs due to latent defects in the software or software-based logic in the DI&C system or component is sufficiently low.

c. Any applicable operating experience regarding the DI&C system or component have been evaluated to provide reasonable assurance that the DI&C system or component will operate with high reliability for the intended application. Operating experience in most cases can serve to compensate for weakness in addressing the other two criteria.

d. The proposed system will not result in a failure that could invalidate the plant licensing basis (e.g., maintaining diverse systems for reactivity control).

5. Spurious Operation Assessment

5.1. Operating Reactors Without IEEE Std 603-1991 as Part of Their Licensing Basis

For proposed DI&C modifications in plants not licensed under IEEE Std 603-1991, the application should include an assessment demonstrating that the spurious operations assumed in the safety analysis are not invalidated by the proposed changes.

Acceptance Criteria

The application includes information that demonstrates the proposed DI&C modification spurious operations assumed in the safety analysis have not been invalidated by the proposed changes.

5.2. Operating Reactors with IEEE Std 603-1991 as Part of Their Licensing Basis or Applications for Construction Permits, Operating Licenses, Standard Design Approvals, Design Certifications, Combined Licenses, or Manufacturing Licenses

Pursuant to the incorporation by reference in 10 CFR 50.55a, IEEE Std 603-1991, Clauses 4.8 and 5.6.3, require that safety-related systems be designed to prevent conditions that can lead to performance degradations of the safety-related system. This includes conditions such as failures or consequential actions by systems that are NSR that could lead to spurious operation of both safety-related components and components that are NSR. For DI&C systems in plants that have IEEE Std 603-1991 as part of their licensing basis or for applications for CPs, OLs, SDAs, DCs, or COLs, the potential for spurious operation resulting from a CCF of the DI&C system should be assessed.

The application should contain an assessment to demonstrate that conditions resulting from potential spurious operation of safety-related components or components that are NSR due to CCF of DI&C systems or components are bounded by events analyzed in the safety analysis. When performing this assessment, the following criteria should be met:

a. The spurious operation should be considered as an initiating event without a concurrent DBE.

b. Design attributes or defensive measures described in Section B.3.1 can be credited in the spurious operation assessment to eliminate further consideration a CCF in an A1 system. Measures described in Section B.4 can be credited to demonstrate the likelihood of CCF of A2 or B1 systems or components is sufficiently low. If the criteria within Section B.3.1 for an A1 system or Section B.4 for an A2 or B1 system are met, then Items c. and d. below are not applicable.

c. In cases that credited design attributes or defensive measures cannot eliminate from further consideration a CCF in an A1 system or the likelihood of CCF in an A2 or B1 system cannot be shown to be sufficiently low, the assessment should determine whether another automatic system or manual operator actions can be credited to mitigate the conditions caused by potential spurious operation of safety-related components or components that are NSR. Section B.3.2 provides criteria on the use of automatic functions and manual operator actions. If the criteria within Section B.3.2 are met, then Item d below is not applicable.

d. For potential spurious operation of safety-related components and components that are NSR due to postulated CCFs that have not been shown to be prevented or mitigated, the following criteria should be used to perform the assessment:

    1. The quality development process of a safety-related DI&C system or components may be credited to reduce the likelihood of CCFs that could lead to spurious operation of a safety function. As such, the assessment should demonstrate that potential spurious operation of a single safety function (e.g., spurious operation of both emergency core cooling system trains) is bounded by the safety analysis.

    2. For discrete digital control systems, the assessment should demonstrate that potential spurious operation of the control functions performed by each discrete digital control system is bounded by the safety analysis.

    3. For highly-integrated DI&C systems that are NSR (e.g., distributed control systems), the assessment should demonstrate that potential spurious operation of multiple functions is bounded by the safety analysis.

    4. The assessment should include evaluation of potential spurious operation of multiple safety-related components or components that are NSR from the use of multi-divisional control and display stations to control these components.

Acceptance Criteria

For I&C systems in plants that have IEEE Std 603-1991 as part of their licensing basis or for applications for CPs, OLs, SDAs, DCs, or COLs, the results of the application should include a documented assessment that provides reasonable assurance to demonstrate the following:

a. Any defensive measures or design attributes implemented for an A1 system to eliminate CCF from further consideration meet the acceptance criteria within Section B.3.1. Any measures implemented for an A2 or B1 system to demonstrate that the likelihood of CCF is sufficiently low meet the acceptance criteria within Section B.4

b. Any automatic functions or manual operator actions credited to mitigate the conditions caused by potential spurious operation of safety-related components or components that are NSR meet the acceptance criteria within Section B.3.2.

c. For those CCFs that have not been shown to be mitigated or prevented, spurious operation of safety-related components or components that are NSR due to a postulated CCF of the DI&C system or component is bounded by the events analyzed in the safety analysis.

6. Manual System Level Actuation and Indications to Address Position 4 of the SRM on SECY-93-087, Item 18.

Displays and manual controls provided for compliance with Position 4 of the SRM on SECY-093-87, Item 18 should be sufficient, both for monitoring the plant state and to enable control room operators to actuate critical safety functions. For DI&C system modifications to operating plants, retention of existing analog displays and controls in the MCR could satisfy this position. However, if existing displays and controls are digital or the same platform is used for mitigating the DBE and to provide signals to these analog displays and controls, this position may not be satisfied.

Once system- or division-level manual actuation from the MCR using the Position 4 displays and controls has been completed, controls outside the MCR for long-term management of these critical safety functions may be used when supported by suitable HFE analysis and site-specific procedures or instructions.

The following criteria should be met for these displays and manual controls:

a. The displays and controls should be sufficient for the operator to monitor and control the following critical safety functions: reactivity level, core heat removal, reactor coolant inventory, containment isolation, and containment integrity.

b. The indication and manual controls to actuate these critical safety functions should be at the system- or division-level and located within the MCR.

c. Equipment that is NSR can be used for these indications and manual controls and indications, provided that the equipment is reliable and of sufficient quality. This equipment should be similar in quality to those required by the ATWS rule (i.e., 10 CFR 50.62), as described in the enclosure to Generic Letter 85-06.

d. The displays and controls should be diverse from the safety-related DI&C systems such that these display and controls are not affected by potential CCFs that could disable the safety-related DI&C systems.

Acceptance Criteria

To reach a conclusion of acceptability of the manual controls and supporting indications to meet Position 4 of the SRM on SECY-93-087, Item 18, the application should demonstrate the following acceptance criteria have been met:

a. The displays and controls are sufficient for the operator to monitor and control the critical safety functions.

b. The manual controls for these critical safety functions are at the system or division level and located within the MCR. Since single failures concurrent with a CCF do not need to be postulated and normal alignment of equipment is assumed, the capability for manual actuation of a single division is sufficient. For plants licensed to allow one division to be continuously out of service, the diverse manual actuation applies to at least one division that is in service.

c. If equipment that is NSR is used, the quality and reliability of the equipment are adequate to support the manual operator actions during the associated event condition.

d. The displays and controls are diverse from the safety-related DI&C systems such that these display and controls are not affected by potential CCFs that could disable the safety-related DI&C systems.

7. Information To Be Reviewed

The information to be reviewed should be commensurate with safety significance of the DI&C system under evaluation. The following information should be reviewed:

a. The documentation of the categorization of a proposed DI&C system and the supporting technical basis for this categorization. If risk insights from plant-specific PRAs are used to inform the categorization, the PRA results should be reviewed.

b. For an A1 system, the results of the D3 assessment, specifically, the following:

    1. Identification of any credited design attribute or defensive measure to eliminate CCF from further consideration and demonstration that these attributes or measures are effective. Identification of any remaining vulnerabilities to potential CCFs.

    2. For CCFs that have not been shown to be eliminated from further consideration through use of design attributes or defensive measures, identification of any diverse means provided to accomplish the same or a different function than the safety function disabled by a potential CCF. If any diverse means are credited to mitigate the potential CCF, the staff should review the information provided to demonstrate the effectiveness of the diverse means, including any HFE analysis associated with manual operator actions as a diverse means.

    3. For CCFs that have not been eliminated from further consideration or mitigated

using diverse means, identification of any analysis performed to demonstrate that consequences due to a potential CCF are within acceptable limits for each AOO or postulated accident. If any consequence analysis has been performed, the staff should review the results of this analysis.

c. For A2 and B1 systems, the results of the qualitative assessment of these systems, specifically, the following:

   1. Information supporting the use of design attributes and features to reduce the likelihood of a CCF such that it is sufficiently low.

   2. Information regarding the quality of the design and development process to reduce the potential for CCFs due to latent defects in the software or software-based logic of the system or component.

   3. Information regarding applicable operating experience to provide reasonable assurance that the DI&C system will operate with high reliability for the intended application.

d. For a B2 system, information provided to show that the proposed design will not introduce any conditions not bounded by the events in the safety analysis due to the specific implementation.

e.

f. Results of the spurious operation assessment for I&C systems in plants that have IEEE Std 603-1991 as part of their licensing basis or for applications for CPs, OLs, SDAs, DCs, or COLs verify on of the following:

   1. Vulnerabilities to potential spurious operations due to a CCF in an A1 system have been addressed through use of design attributes or defensive measures to prevent, limit or mitigate the consequence of a CCF;

   2. Vulnerabilities to potential spurious operations due to a CCF in an A2 or B1 system have been addressed through use of a combination of the three factors described in Section B.4; or

   3. The consequence of a potential spurious operation due to a CCF is bounded by the safety analysis;

g. For a proposed A1 system, design information provided to verify that controls and displays:

   1. Have been provided in the MCR to perform manual system or division level actuation of critical safety functions.

   2. Are diverse from the A1 system such that they are not subject to the same CCF as the A1 system.

3. Have adequate quality to support the manual operator actions during the associated event condition if the equipment used is NSR..

8. Review Procedures

In reviewing the D3 assessment results in accordance with the acceptance criteria described in Section B.3 of this BTP and the detailed guidance of NUREG/CR-6303, emphasis should be given to the topics described below:

8.1. System Representation as Blocks

The system being assessed is represented as a block diagram; the inner workings of the blocks are not necessarily shown. Diversity is determined at the block level. A block is a physical subset of equipment and software for which it can be credibly assumed that internal failures, including the effects of software and logic errors, will not propagate to other equipment or software. A block can be a software macro/subroutine, such as voting block or proportional-integral-derivative block, that is used by multiple functional applications; a design or implementation defect in this type of block can result in a CCF of all application functions that utilize that block.

Examples of typical blocks are computers, local area networks, software macros/subroutines, and programmable logic controllers.

8.2. Documentation of Assumptions

Assumptions made to compensate for missing information in the design description materials or to explain particular interpretations of the analysis guidelines as applied to the system are documented by the applicant.

8.3. Effect of Other Blocks

When considering the effects of a postulated CCF, diverse blocks are assumed to function correctly. This includes the functions of blocks that act to prevent or mitigate consequences of the CCF under consideration.

8.4. Identification of Alternate Trip or Initiation Sequences

Thermal-hydraulic analyses using realistic assumptions of the sequence of events that would occur if the primary trip channel failed to trip the reactor or actuate ESF are included in the assessment. Coordination with the organization responsible for the review of reactor systems is necessary in reviewing these analyses.

8.5. Identification of Alternative Mitigation Capability

For each DBE, alternate mitigation actuation functions that will prevent or mitigate core damage and unacceptable release of radioactivity should be identified. When a CCF in an automatic or manual function credited in the plant safety analysis is compensated by a different automatic or manual function, a basis should be provided that demonstrates that the different function

constitutes adequate mitigation for the conditions of the event.

When operator action is cited as the diverse means for response to an event, the applicant should demonstrate that adequate information (indication), appropriate operator training, and sufficient time for operator action are available in accordance with SRP Chapter 18. Coordination with the organization responsible for the review of human-system interfaces for any diverse credited manual operator actions should be included as part of this activity.

8.6. Justification for Not Correcting Specific Vulnerabilities

If any identified vulnerabilities are not addressed by aspects such as design attributes, defensive measures, or provision of alternate trip, initiation, or mitigation capability, justification should be provided. This includes any NRC-approved credited operator actions taken to prevent the AOO or postulated accident from occurring. These justifications will be reviewed on a case-by-case basis.

C. REFERENCES

1. Institute of Electrical & Electronics Engineers, IEEE 100, “The Authoritative Dictionary of Standards Terms,” Piscataway, NJ.

2. Institute of Electrical & Electronics Engineers, IEEE Std 279-1968, “Proposed IEEE Criteria for Nuclear Power Plant Protection Systems,” Piscataway, NJ.

3. Institute of Electrical & Electronics Engineers, IEEE Std 279-1971, “Criteria for Protection Systems for Nuclear Power Generating Stations,” Piscataway, NJ.

4. Institute of Electrical & Electronics Engineers, IEEE Std 379-2000, “IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems,” Piscataway, NJ.

5. Institute of Electrical & Electronics Engineers, IEEE Std 603-1991, “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations,” Piscataway, NJ.

6. Institute of Electrical & Electronics Engineers, IEEE Std 603-1991, “Standard Criteria for Safety Systems for Nuclear Power Generating Stations,” Correction Sheet, January 30, 1995.

7. U.S. Nuclear Regulatory Commission, “A Defense-in-Depth and Diversity Assessment of the RESAR-414 Integrated Protection System,” NUREG-0493, March 1979.

8. U.S. Nuclear Regulatory Commission, “Application of the Single-Failure Criterion to Safety Systems,” Regulatory Guide 1.53.

9. U.S. Nuclear Regulatory Commission, “Control Systems,” NUREG-0800, SRP Section 7.7.

10. U.S. Nuclear Regulatory Commission, “Digital Computer Systems for Advanced Light-Water Reactors,” SECY-91-292, September 16, 1991.

11. U.S. Nuclear Regulatory Commission, “Diverse Instrumentation and Control Systems,” NUREG-0800, SRP Section 7.8.

12. U.S. Nuclear Regulatory Commission, “Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems,” NUREG/CR-7007, December 2008.

13. U.S. Nuclear Regulatory Commission, “Human Factors Engineering,” NUREG-0800, SRP Chapter 18.

14. U.S. Nuclear Regulatory Commission, “Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems,” NUREG/CR-6303, December 1994.

15. U.S. Nuclear Regulatory Commission, “Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs,” SECY-93-087, April 2, 1993.

16. U.S. Nuclear Regulatory Commission, “Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs,” SRM for SECY-93-087, July 21, 1993.

17. U.S. Nuclear Regulatory Commission, “Plan for Addressing Common Cause Failure in Digital Instrumentation and Controls,” SECY-18-0090, September 12, 2018.

18. U.S. Nuclear Regulatory Commission, “Quality Assurance Guidance for ATWS Equipment That Is Not Safety-Related,” Generic Letter 85-06, April 16, 1985.

19. U.S. Nuclear Regulatory Commission, Regulatory Issue Summary 2002-22 Supplement 1, “Clarification on Endorsement of Nuclear Energy Institute Guidance in Designing Digital Upgrades in Instrumentation and Control Systems,” May 31, 2018.

Paperwork Reduction Act Statement

This Standard Review Plan provides voluntary guidance for implementing the mandatory information collections in 10 CFR Parts 50 and 52 that are subject to the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et. seq.). These information collection were approved by the Office of Management and Budget (OMB), approval numbers 3150-0011 and 3150-0151. Send comments regarding this information collection to the Information Services Branch (T6-A10M), U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001, or by e-mail to Infocollects.Resource@nrc.gov, and to the OMB reviewer at: OMB Office of Information and Regulatory Affairs (3150-0011, 3150-0151), Attn: Desk Officer for the Nuclear Regulatory Commission, 725 17th Street, NW Washington, DC 20503; e-mail: oira_submission@omb.eop.gov.

Public Protection Notification

The NRC may not conduct or sponsor, and a person is not required to respond to, a collection of information unless the document requesting or requiring the collection displays a currently valid OMB control number.

BTP Section 7-19

Description of Changes

BTP 7-19, "GUIDANCE FOR EVALUATION OF POTENTIAL COMMON CAUSE FAILURE IN DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS"

This BTP section updates the guidance previously provided in Revision 7, dated August 2016 (Agencywide Documents and Management System (ADAMS) Accession No. ML16019A344).

The main purpose of this update is to provide clarification on sections of the guidance that proved challenging to implement based upon feedback received by internal and external stakeholders. This update improves readability and the flow of information such that it is clear to the reader that there is an established process for analyzing for potential hazards caused by CCFs of digital technology, in particular within software. This update clarifies the scope of applicability for all users as well as clearly stating the applicability of this guidance to the 10 CFR 50.59 change process. The update provides for a graded approach that clarifies the technical rigor and analysis that's appropriate for SSCs of differing safety class so that an adequate demonstration of safety for a proposed is consistently applied. This is in addition to clarifying specific areas of guidance such as with regard to diversity and testing to eliminate further consideration of CCF. Lastly, the update revises the flow and structure of the BTP's guidance to improve readability so that the user clearly understands the overall process for addressing CCF, which correlates to the graded approach methodology.