U.S. NUCLEAR REGULATORY COMMISSION

STANDARD REVIEW PLAN

BRANCH TECHNICAL POSITION 7-19

GUIDANCE FOR EVALUATION OF COMMON CAUSE FAILURE HAZARDS 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 – January 2020

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 regulations (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 ability to integrate design functions using DI&C technology and its inherent complexity compared to analog technologies. DI&C systems or components can be vulnerable to a CCF due to defects in hardware or to latent defects in the software or software-based logic. Latent defects in hardware, software, or system components within redundant portions (e.g., safety divisions[1]) of a safety-related system can be triggered by an event or condition and thus lead to a systematic fault. A CCF hazard[2] (e.g., loss of the capability to perform a safety function) can result from the occurrence of such a systematic fault during a design-basis event (DBE). This BTP is focused on addressing CCF hazards resulting from systematic faults caused by latent defects in the software or software-based logic. [3]

A CCF of a DI&C system or component can also initiate the operation of 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, 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-414 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 discussed its concerns about CCF hazards 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 hazards 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

[1] This BTP uses the term "division" as defined in IEEE Std 603-1991.
[2] If a CCF as a result of a systematic fault due to latent defects does not disable a safety function credited to mitigate a DBE, then the occurrence of this CCF is not considered a CCF hazard. The term "hazard" is defined as potential for harm, which in this context means disabling of the safety function or causing unmitigated initiating events resulting from spurious operation of safety functions or other design functions.
[3] Other types of CCF hazards can exist and are addressed in other staff review guidance.

(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 CCF hazards of a DI&C system are considered beyond-design-basis events.

The NRC staff provided plans to the Commission to clarify the guidance associated with addressing CCF hazards 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 CCF hazards 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 CCF hazards due to software in DI&C systems to be beyond design basis, the application should include an evaluation of CCF hazards due to software in DI&C systems and should verify that the plant is protected from the effects of these CCF hazards. In addition, the application should include an evaluation of sources of this CCF hazard 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 CCF hazards in DI&C systems. During these reviews, the NRC staff has observed that different solutions may be used to address CCF hazards, and that one standard solution may not be applicable to all DI&C systems. This BTP provides guidance for reviewing the design and analysis for addressing CCF hazards due to latent software defects in DI&C systems.

1. Regulatory Basis

The regulations listed below may not necessarily apply to all 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 NPPs with CPs issued before January 1, 1971, Title 10 of the *Code of Federal Regulations* (10 CFR) 50.55a(h), "Protection and Safety Systems," requires compliance with the plant-specific licensing basis or IEEE Std 603-1991 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 applications for construction permits (CPs), operating licenses (OLs), combined licenses (COLs), standard design approvals (SDAs), design certifications (DCs), filed after May 13, 1999, 10 CFR 50.55a(h) 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.

- 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 [Clause] 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 licensees of 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 protection system design shall ensure "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 the requirement to address CCF hazards and for requiring the use of 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, for which the licensee has 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 CCF hazards concurrent with a DBE.

- 10 CFR 50.67 provides guideline values for fission product releases from currently operating NPPs for which the licensee has implemented an alternative source term.

- 10 CFR 50.34(a)(1)(ii)(D) provides site dose guideline values for CP applications filed under 10 CFR Part 50 after January 10, 1997.

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

- 10 CFR 52.79(a)(1)(vi) provides site dose guideline values for COL applications.

- 10 CFR 52.137(a)(2)(iv) provides side dose guideline values for SDA applications.

- 10 CFR 52.157(d) provides site dose guideline values for ML applications.

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[4] that could occur within digital RPSs and determines what portions of a design need to implement additional D3 measures to address such failures.

- 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 vulnerabilities that can lead to a CCF hazard. NUREG/CR-7007 identifies and develops a baseline set of diversity criteria that may constitute appropriate mitigating diversity strategies to address potential vulnerabilities to CCF hazards. 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.

- SECY-18-0090 provides the NRC staff's plan to clarify the guidance associated with evaluating and addressing CCF hazards 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 hazard.

- 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.

[4] It should be noted that while these documents use the term "common-mode failure," the term "common-cause failure" is used in this BTP because it better characterizes this type of failure.

- 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 hazards.

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

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 to 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 an evaluation of (1) a DI&C system’s vulnerability to a CCF hazard due to latent defects in the software or software-based logic, (2) any diverse means credited to address remaining vulnerabilities to a CCF hazard, and (3) the effects of any unmitigated vulnerabilities to a CCF hazard on plant safety. This BTP also provides guidance on implementing a graded approach to address CCF hazards 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,[5] and logic developed from software-based development systems (e.g., hardware description language programmed devices).

This BTP is intended to address an applicant’s approach to address CCF hazards caused by latent defects in the software or software-based logic. This type of CCF hazard is considered a beyond-design-basis event for structures, systems, and components (SSCs) that employ a robust design process to reduce the likelihood of design defects. The plant response to these beyond-design-basis events 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 hazard (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 analyzed using conservative methods to demonstrate that the plant response to these events is bounded by the events in the accident

[5] 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.

analysis section of the SAR. RG 1.53 provides guidance for the deterministic analysis of single failures in safety-related systems.

This BTP provides guidance for reviewing (1) design attributes, such as the use of diverse equipment within a system or component to eliminate the CCF hazard from further consideration,[6] (2) diverse external equipment, including manual controls and displays to mitigate a CCF hazard, and (3) other measures to ensure conformance with the NRC's position on addressing CCF hazards 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 a CCF hazard 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 conducted and meets the acceptance criteria described in this BTP. An adequate D3 assessment consists of
    - An evaluation of vulnerabilities to a CCF hazard due to latent defects in system and the effectiveness of any credited attributes to eliminate the CCF hazard from further consideration;
    - Identification of any credited diverse means to mitigate CCF hazards that have not been eliminated from further consideration and the evaluation of the effectiveness of these diverse means; and
    - An assessment of the consequences of residual CCF hazards that have not been eliminated from further consideration or mitigated to demonstrate that the consequences remain bounded[7] by the events analyzed in the accident analyses.
- A qualitative assessment of proposed DI&C systems of lower safety significance obtains results that meet the acceptance criteria within this BTP.

This BTP also addresses the applicant's assessment of vulnerabilities to a CCF hazard due to latent software defects that can cause the spurious operation of a safety-related component or a component that is NSR, because such spurious operations have the potential to put the plant in a condition that has not been previously analyzed in the accident 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 reviewing an applicant's assessment of CCF hazards of DI&C systems that can result in spurious operation of safety-related components or components that are NSR.

B. BRANCH TECHNICAL POSITION

1. Introduction

[6] The description of how a CCF hazard is eliminated from further consideration is discussed in Section B.3.1 of this BTP.
[7] The term "bounded" as used in the BTP means that the plant conditions remain within the acceptance criteria of the events analysis in the accident analysis.

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 a D3 assessment to demonstrate that vulnerabilities to CCF hazards have been adequately addressed. The guiding principles within SECY-18-0090 clarify that it is acceptable to use a graded approach commensurate with the safety significance of the proposed DI&C system or component to determine the degree of rigor that is necessary to address CCF hazards. 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" (i.e., "realistic assumptions") 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, it is acceptable to use either realistic assumptions to analyze the plant response to DBEs, or the conservative assumptions on which the accident analysis based. Each event analyzed within the accident 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 shows a postulated CCF could disable a safety function (i.e., become a CCF hazard), then Position 3 directs the assessment to 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 hazard. 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 CCF hazards. 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 CCF hazard, when evaluated in the accident analysis can be reasonably mitigated through other means (such as with current systems), a 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 hazard that disabled the safety function.

If a diverse means is part of a safety-related system, 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 "non-safety") in the main control room (MCR) that is diverse from any vulnerability to a CCF hazard 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 "non-safety," these terms in context refer to safety-related and NSR SSCs, respectively. Depending on the design, these displays and controls should provide manual system or divisional level 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[8] may be credited as all or part of the diverse means provided to address Position 3.

The Position 4 phrase "safety computer system identified in Items 1 and 3 above" refers to a safety-related DI&C system that is credited for mitigating an AOO or postulated accident in the

[8] SECY-18-0090 did not provide any clarification for Position 4.

accident 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, acknowledge that DI&C system development errors (i.e., latent defects) are a credible source of CCF hazards. 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, DI&C systems may be vulnerable to CCF hazards if 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, terms such as "higher-level requirements" do not refer to NRC regulatory requirements but to system or component design or operating characteristics that are relied upon to accomplish the stated system or component functions. Throughout this BTP, context indicates whether requirements are NRC regulatory requirements.

SECY-18-0090 recognizes that, although significant effort has been applied to the development of highly reliable DI&C systems, some residual faults may remain undetected within a system and could result in CCF hazards that can challenge plant safety. This includes CCF 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 CCF hazards, the NRC staff should verify that for each event analyzed in the accident analysis section of the SAR, the application has:

- Identified vulnerabilities to CCFs due to a design or implementation defect in a DI&C system and evaluated the impacts of these postulated CCFs to safety functions or other design functions to determine whether these postulated CCFs can lead to a hazard;
- Demonstrated that a CCF hazard 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
- Assessed the ability of the overall plant design (e.g., I&C systems, mechanical systems, and manual operator action) to maintain plant safety, using conservative or "best estimate" methods, for those CCF hazards 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 SAR 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

This BTP adopts a graded approach, described in Table 2-1, for determining how to address CCF hazards based on the safety category and significance of the SSC. For assessing vulnerabilities to CCF hazards, a graded approach refers to analyses performed for equipment of differing safety significance in which CCF hazard concerns apply.

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

	Safety-Related	Not Safety-Related

Safety Significant A significant contributor to plant safety	**A1 DI&C SSCs** Relied upon to initiate and complete control actions essential to maintain plant parameters within acceptable limits established for a DBE. **or** Failure could directly lead to accident conditions that may cause unacceptable consequences (i.e., exceeds siting dose guidelines for a DBE) if not mitigated by other A1 systems. **Application should include a D3 assessment as described in Section B.3**	**B1 DI&C SSCs** 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** Failure may result in unacceptable consequences to plant safety due to integration of multiple control functions into a single system. **Application should include a qualitative assessment as described in Section B.4**
Not Safety Significant Not a significant contributor to plant safety	**A2 DI&C SSCs** Provides an auxiliary or indirect function in the achievement or maintenance of plant safety. **or** Maintains the plant in a safe shutdown state after the plant has reached initial safe shutdown state.[9] **Application should include a qualitative assessment as described in Section B.4**	**B2 DI&C SSCs** Does not have a direct effect on reactivity or power level of the reactor or affect the integrity of the safety barriers (fuel cladding, reactor vessel, or containment). **and** Failure does not have consequences to plant safety or whose failure can be detected and mitigated with significant safety margin. **Application may need to include a qualitative assessment as described in Section B.4** if the proposed design could introduce conditions[10] that have not been previously analyzed in the SAR.

For example, an assessment of CCF hazards for a digital RTS would be expected to be more rigorous than an assessment of CCF hazards 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 shut down the plant, if necessary.

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.

[9] The plant safe shutdown state is site-specific, as defined in the particular facility's licensing basis.
[10] For example, newly combined design functions, shared resources, or connectivity to other plant systems.

The graded approach presented in Table 2-1 is 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.”

System integration and interconnectivity among the categories identified in Table 2-1 can introduce additional vulnerabilities to CCF hazards. 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 CCF hazards of the integrated system and the consequences of these CCF hazards 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 performs 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 Sections B.3.1 through B.3.3 for an A1 system apply to these interconnected or integrated systems.

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

A D3 assessment is necessary for a proposed A1 system or component to determine whether vulnerabilities to CCF hazards have been adequately addressed. For each event analyzed in the accident analysis section of the safety analysis report, the results of the D3 assessment should show that vulnerabilities to CCF hazards have been adequately addressed through any combination of the following:

a. CCF hazard has been eliminated from further consideration per the criteria within Section B.3.1;

b. CCF hazard has been adequately mitigated, per the criteria within Section B.3.2, using a diverse means for performing the same or different function than the safety function postulated to be disabled by the CCF; or

c. The consequences of the CCF hazard are acceptable for the associated DBE per the acceptance criteria within Section B.3.3.

The applicant may elect to apply any combination of the above three methods to the entire A1 system or portions of the A1 system. For example, the applicant may show that the CCF hazard has been eliminated for a component within the A1 system and exclude this component when addressing the CCF hazard for the rest of the A1 system.

The adequacy of the D3 assessment, including any (1) measures used to eliminate the CCF hazard from further consideration, (2) diverse means provided to mitigate the CCF hazard, or (3) analysis to show the consequences of the CCF hazard are acceptable for each DBE, should be justified in the application and explicitly addressed in the NRC staff’s safety evaluation.

3.1. Means to Eliminate Common-Cause Failure Hazard from Further Consideration

Many system design and testing attributes, procedures, measures, and practices can contribute to significantly reducing the likelihood of a CCF hazard. However, there are certain design attributes that are sufficient to eliminate from further consideration a CCF hazard due to a digital design or implementation defect. These attributes include (1) diversity within the DI&C system or component, (2) testability, and (3) defensive measures within the design. Although these attributes do not eliminate the CCF hazard completely, the residual risk for a CCF hazard is minimized such that no further evaluation is necessary. The basis for the acceptability of this residual risk is discussed for each attribute in the subsections below.

If the application demonstrates that use of these attributes for an A1 system or component meet the criteria within this BTP, then the CCF hazard has been eliminated from further consideration. Thus, 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 a CCF of the proposed A1 system does not need to be performed for the portion of the A1 system or component that credit these attributes.

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

If sufficient diversity exists within each safety division or among redundant safety divisions of an A1 system to perform the safety function, then the CCF hazard can be eliminated from further consideration. For example, a digital protection system could be designed such that each credited safety function is implemented in one division of the protection system that uses one type of digital technology and another division that uses a different type of digital technology. In this case, the application should include an analysis using the guidance of NUREG/CR-6303 and NUREG/CR-7007 to demonstrate that the diversity attributes between these two divisions of the digital protection system are adequate to eliminate a CCF hazard such that further consideration is unnecessary. Given that this analysis is qualitative in nature, the potential that a CCF hazard can affect both diverse divisions is minimized but not eliminated. However, the potential of a CCF hazard due to latent defects in the software of the diverse portions is much lower than failures that are considered in the accident analysis (e.g., single failures) and comparable to other CCF hazards that are not considered in the accident analysis (e.g., design flaws, maintenance errors, calibration errors).

It should be noted that because each redundant safety-related division is credited for compliance with the single-failure criterion and is now additionally credited to prevent the CCF hazard, 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. The consistency of proposed changes and technical specifications should be addressed in the application.

Acceptance Criteria

The reviewer should reach a conclusion that the application provides adequate information on the use of diversity within the A1 system or component to eliminate CCF hazards from further consideration, if the application demonstrates the following acceptance criteria are met:

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

b. An analysis demonstrates that adequate diversity has been achieved between the diverse portions of the A1 system or component in accordance with the guidance of NUREG/CR-6303 and NUREG/CR-7007.

c. 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 portions. The diverse portions of the A1 system or component do not share engineering or maintenance tools that could affect both portions.

d. Each diverse portion 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.

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

f. Consistency is maintained between the proposed change and technical specifications.

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

When considering CCF hazards in DI&C systems or components, there are two general areas of concern: (1) CCF hazards as a result of errors introduced by the system or software requirements, and (2) CCF hazards as a result of errors introduced during the design and implementation of the software or software-based logic. A quality development process can be credited to address potential errors in the system or component requirements or specifications for both analog and digital equipment. However, the quality of the development process cannot eliminate potential defects introduced during the design and implementation process. Testing can identify latent defects that could lead to a CCF hazard in the design, fabrication, and implementation of software or software-based logic. Testing can be used to both identify latent defects for correction in the design, fabrication, and implementation process and to demonstrate that any potential latent defects have been corrected.

If testing of a proposed A1 component shows that there are no potential latent defects of the component software or software-based logic, then the CCF hazard can be eliminated from further consideration. As discussed above, since testing only eliminates potential latent defects introduced during the design, fabrication, and implementation of the component, a CCF hazard could still occur as a result of errors in the system or component requirements specifications. However, a quality development process can minimize such errors and the potential for such residual errors is the same for both analog and digital components.

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. For this testing to effectively represent the operational conditions expected for the

component under test, this testing should be performed under anticipated operational conditions of the proposed A1 component. To credit testing as a means of demonstrating that 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 that any credited testing includes the following:

a. The combination of every possible input. Any unused inputs to the component that will be permanently forced to a fixed state can be set at that fixed state. The design does not include any analog input.

b. If 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.

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 either all possible past condition sequences should be included in the testing or the past condition sequences should be shown through analysis to not affect the device output.

d. Any logic or circuits that are not used under any operational condition can be excluded from the test cases if 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.

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

The reviewer should reach a conclusion that the application provides adequate information on the test results and testing methodology for a device or component such that a CCF hazard can be eliminated from further consideration, if the application demonstrates the following acceptance criteria are 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. Any application that excludes from the test cases logic or circuits of devices or

components, because they are not used under any operational condition, has demonstrated that the logic or circuits excluded do 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 Common-Cause Failure Hazard from Further Consideration

Defensive measures may be used to prevent, limit, or mitigate the effects of a CCF hazard. If the application credits the use of such defensive measures to eliminate a CCF hazard 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 CCF hazard will be prevented, limited, or mitigated by the proposed defensive 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 CCF hazard 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 CCF hazards

If an application (e.g., license amendment request, request for NRC approval of industry guidance, or request for design certification) credits use of defensive measures to eliminate CCF hazards from further consideration, the defensive measures being credited, along with a supporting technical basis and acceptance criteria, should be based upon an NRC-approved methodology or otherwise described as part of the application.

Acceptance Criteria

The reviewer should reach a conclusion that the application provides sufficient information on the credited defensive measures to eliminate a CCF hazard from further consideration if the application includes the documented supporting technical basis and acceptance criteria to demonstrate that these defensive measures are based on an NRC-approved methodology. If a technical basis and acceptance criteria are submitted in the application, the NRC staff will review the information on a case-by-case basis.

3.2. Use of Diverse Means to Mitigate Common-Cause Failure Hazards

If a CCF hazard has not been eliminated from further consideration using the process in Section B.3.1 of this BTP, a diverse means should be provided to accomplish the same or different

function than the safety function disabled by the postulated CCF. An application that credits any of the diverse means described in Sections B.3.2.1 through B.3.2.3 are considered acceptable to address Position 3 of the SRM on SECY-93-087, Item 18. These diverse means include crediting existing systems, crediting manual operator action, or crediting a diverse system. The application should demonstrate the following:

a. Any credited existing system(s) are capable of effectively performing the same or a different function in response to the DBE

b. Any manual operator action(s) credited in the D3 assessment are capable of responding with sufficient time available for the operators to determine the need for manual operator action, even with indicators that may be malfunctioning due to the CCF hazard

c. Any credited diverse system(s) are supported by sufficiently independent instrumentation that indicates

    1. whether the safety function is needed,
    2. whether the A1 system did not perform the safety function, and
    3. whether the automated diverse means or manual operator action is successful in performing the design functions necessary to mitigate the CCF hazard.

3.2.1. Crediting Existing Systems

An existing highly reliable I&C system can be used as a diverse means to provide the same or a different function credited in the D3 assessment. 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 report. 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. NUREG/CR-7007 identifies and develops a baseline set of diversity criteria that may constitute appropriate mitigating diversity strategies to address vulnerabilities to CCF hazards.

The existing system may be a system that is NSR provided it is of sufficient quality and can reliably perform the credited 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

The reviewer should reach a conclusion that the application includes a D3 assessment

acceptable to justify the use of an existing plant system as the diverse means used to perform the same function disabled by a postulated CCF or to perform a different function to compensate for or mitigate the loss of the function disabled by a postulated CCF if the application demonstrates the following acceptance criteria are 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 application should show that the capabilities for sensing and responding maintain plant safety by verifying plant conditions stay within the acceptance criteria specified for each AOO or postulated accident in the safety analysis report.

3.2.2. Crediting Manual Operator Action

Manual operator action that can be performed within an acceptable time frame, as defined in SRP Chapter 18, can be used as a diverse means to provide the same or a different function credited in the D3 assessment. If manual operator action is used as the diverse means, the equipment necessary to perform such action, including the supporting indications, should be diverse and independent from the safety-related I&C system disabled by a postulated CCF. If the equipment used to perform the credited manual operator action is NSR, then the application should include information to demonstrate that the equipment used is highly reliable and of sufficient quality. This equipment should be similar in quality to that 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 hazard that affects normal displays or controls should not prevent the operator from manually performing the safety functions.

The application should contain an HFE analysis in accordance with the guidance of SRP Chapter 18, to demonstrate that plant conditions can be maintained within specified acceptance criteria for the particular AOO or postulated accident. The credited manual operator action and the equipment necessary to perform the action should be identified. If equipment outside of the MCR is used to perform the credited manual operator action, 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

The reviewer should reach a conclusion that the application includes a D3 assessment acceptable to justify the use of manual operator action as the diverse means used to perform the same or a different function as the safety function disabled by the postulated CCF, if the application demonstrates the following acceptance criteria are met:

a. The manual operator action can be performed within an acceptable time frame as specified in SRP Chapter 18. The difference between the time available to perform the operator action, as determined by the thermal-hydraulic analysis, and the time necessary to perform it, as determined by the HFE analysis, 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 reliably perform the action within the time available. For complex situations and for manual operator action with limited margin between time available and time necessary, 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, can be used as a diverse means to provide the same or a different function credited in the D3 assessment. If such a system is credited as a diverse means to address CCF hazards, the application should demonstrate that (1) the functions performed by this diverse means are adequate to maintain plant conditions within specified acceptance criteria for the associated DBE and (2) sufficient diversity exists between this diverse system and the A1 system such that a postulated CCF cannot disable both systems. 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 CCF hazard. 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

The reviewer should reach a conclusion that the application includes a D3 assessment acceptable to justify the use of the diverse system as the diverse means used to perform the same or a different function as the safety function disabled by the postulated CCF, if the application demonstrates the following acceptance criteria are met:

a. The functions performed by the diverse system are adequate to maintain plant conditions within the specified acceptance criteria for the associated DBEs.

b. Sufficient diversity exists between the diverse system and the A1 system such that a postulated CCF cannot disable both systems.

c. The equipment to be credited has functional capabilities ~~characteristics~~ sufficient to maintain the plant within the applicable acceptance criteria.

d. Any use of priority functions to prioritize commands from the diverse system and the A1 system or other systems/manual operator action has been shown to ensure that the highest priority commands (1) direct components to a safe state, or (2), for those components with multiple safe states, direct components to the state that minimizes consequences to plant safety. The basis for the priority ranking should be documented.

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.

3.3. Consequences of the CCF Hazard Are Acceptable

For each event analyzed in accident analysis, 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. This assessment should show that consequences of CCF hazards of an A1 or portions of an A1 system are acceptable per the acceptance criteria below.

Acceptance Criteria

The reviewer should reach a conclusion that the application provides adequate information to show that consequences of CCF hazards of an A1 or portions of an A1 system are acceptable if the application shows the following acceptance criteria are met:

a. For each AOO in the design basis occurring in conjunction with the CCF hazard, 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.

b. 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).

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 an 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) such that likelihood of failure of the proposed DI&C system is consistent with the assumptions in the SAR. 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 CCF hazards 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 CCF hazards 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 hazard 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 SAR. This approach can also be used for a new reactor design.

The reviewer should reach a conclusion that the application has addressed a CCF hazard in A2, B1, or applicable B2 systems if the application provides a qualitative assessment demonstrating the likelihood of the CCF hazard is sufficiently low based on any of the following criteria :

a. Design attributes and features of the proposed system that reduce the likelihood of CCF hazards.

b. Quality of the design process of the DI&C system that reduces the likelihood for CCF hazards due to latent defects in the software or software-based logic in the DI&C system or component.

c. The applicable operating experience regarding the DI&C system or component collectively supports a conclusion 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 Not Required To Address IEEE Std 603-1991

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 accident analysis are not invalidated by the proposed modification to the DI&C system.

Acceptance Criteria

The reviewer should reach a conclusion that the application includes adequate information on the results of the spurious operation assessment if the application demonstrates the spurious operation of safety-related components or components that are NSR assumed in the accident analysis have not been invalidated by the proposed modification of the DI&C system or component.

5.2. IEEE Std 603-1991 Applies

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, COLs, or MLs, the potential for spurious operation resulting from a CCF hazard of

the DI&C system should be assessed using the following considerations:

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

b. For an A1 system, potential spurious operation of safety-related components or components that are NSR due to CCF hazards can be adequately addressed through any combination of the following:

   1. CCF hazard has been eliminated from further consideration per the criteria within Section B.3.1;

   2. CCF hazard has been adequately mitigated, per the criteria within Section B.3.2, using a diverse means to mitigate the initiating event created by the spurious operation of components; or

   3. The consequences of the initiating event created by the spurious operation of safety related components or components that are NSR are acceptable per the acceptance criteria within Section B.3.3.

      i When applying the acceptance criteria within Section B.3.3, whether the initiating event created by the CCF hazard is considered an AOO or postulated accident should be justified and documented in the application.

      ii The quality development process of an A1 system or components may be credited to reduce the likelihood of CCF hazards that could lead to spurious operation of a safety function. As such, the application should demonstrate that the initiating event created by potential spurious operation of a single safety function (e.g., spurious operation of both emergency core cooling system trains) is bounded by the accident analysis.

c. For an A2 or B1 system, potential spurious operation of safety-related components or components that are NSR due to CCF hazards can be adequately addressed through any combination of the following:

   1. Likelihood of CCF hazards are reduced to “sufficiently low” level using the measures described in Section B.4

   2. CCF hazard has been adequately mitigated, per the criteria within Section B.3.2, using a diverse means to mitigate the initiating event caused by spurious operation of components;

   3. The consequences of the initiating event created by the spurious operation of safety related components or components that are NSR are acceptable per the acceptance criteria within Section B.3.3.

      i When applying the acceptance criteria within Section B.3.3, whether the initiating event created by the CCF hazard is considered an AOO or postulated accident should be justified and documented in the application.

      ii For highly-integrated B1 systems (e.g., distributed control systems), the application should demonstrate that potential spurious operation of multiple functions is bounded by the accident analysis.

iii For discrete B1 systems, the application should demonstrate that potential spurious operation of the control functions performed by each discrete B1 system is bounded by the accident analysis.

iv The analysis of potential spurious operation should include A2 or B1 systems that are considered multi-divisional control and displays.

Acceptance Criteria

The reviewer should reach a conclusion that the spurious operation assessment results are acceptable if the application demonstrates the following acceptance criteria are met:

a. Any defensive measures or design attributes implemented for an A1 system to eliminate CCF hazard from further consideration meet the acceptance criteria within Section B.3.1.

b. Any measures implemented for an A2 or B1 system to demonstrate that the likelihood of CCF hazard is sufficiently low meet the acceptance criteria within Section B.4.

c. Any automatic functions or manual operator action 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.

d. For those CCF hazards that have not been shown to be mitigated or prevented, consequences resulting from spurious operation of safety-related components or components that are NSR are bounded by the events analyzed in the accident 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 to monitor 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 Position 4. However, if existing displays and controls are digital, or the same platform is used both for mitigating the DBE and to provide signals to these analog displays and controls, retaining existing analog displays and controls may not be sufficient to meet Position 4.

For displays and manual controls used to conform to Position 4, the following criteria should be met:

a. The displays and controls should be sufficient for the operator to monitor and control the following critical safety functions: reactivity, 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 may be used for these manual controls and indications, provided that the equipment is reliable and of sufficient quality. This equipment should be similar

in quality to that 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 that are vulnerable to a CCF hazard such that these display and controls are not affected by potential CCFs that could disable the safety-related DI&C systems.

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.

Acceptance Criteria

The reviewer should reach a conclusion that the manual controls and supporting indications conform to Position 4 of the SRM on SECY-93-087, Item 18, if the application demonstrates 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 action during the associated event condition.

d. The displays and controls are diverse from the safety-related DI&C systems such that these displays and controls are not affected by postulated CCFs that could disable the safety functions performed by 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 hazards from further consideration and a demonstration that these

attributes or measures are effective. Identification of any remaining vulnerabilities to CCF hazards.

2. For CCF hazards that have not been eliminated from further consideration, identification of any diverse means provided to accomplish the same or a different function than the safety function disabled by a postulated CCF. If any diverse means are credited to mitigate the CCF hazard, the NRC staff should review the information provided to demonstrate the effectiveness of the diverse means, including any HFE analysis associated with manual operator action as a diverse means.

3. For CCF hazards that have not been eliminated from further consideration or mitigated using diverse means, identification of any analysis performed to demonstrate that consequences of a CCF hazard are within acceptable limits for each AOO and postulated accident. If any consequence analysis has been performed, the NRC 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 hazard such that it is sufficiently low.

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

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

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

e. Results of the spurious operation assessment, for I&C systems in NPPs to which IEEE Std 603-1991 applies, specifically, information showing the following:

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

2. Vulnerabilities to potential spurious operations due to a CCF hazard 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 hazard is bounded by the accident analysis;

f. For a proposed A1 system, design information showing 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 hazard as the A1 system; and

3. Have adequate quality to support the manual operator action 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 and NUREG/CR-7007, 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. 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 hazard of all application functions that utilize that block. Diversity is determined at the block level.

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

8.2. Documentation of Assumptions

The application documents any assumptions made to compensate for missing information in the design description materials or to explain interpretations of the analysis guidelines as applied to the system.

8.3. Effect of Other Blocks

Diverse blocks are assumed to function correctly when considering the effects of a CCF hazard. This includes the functions of blocks that act to prevent or mitigate consequences of the CCF hazard under consideration.

8.4. Identification of Alternate Trip or Initiation Sequences

The assessment includes 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. 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 hazard in an automatic or manual function credited in the plant accident 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 the HFE analysis is adequate in accordance with SRP Chapter 18. Coordination with the organization responsible for the review of human-system interfaces for any credited diverse manual operator action should be included as part of this activity.

8.6. Justification for Not Correcting Specific Vulnerabilities

Justification should be provided for not correcting any identified vulnerabilities not addressed by other aspects of the application such as design attributes, defensive measures, or provision of alternate trip, initiation, or mitigation capability. This includes any NRC-approved credited operator action 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 COMMON CAUSE FAILURE HAZARDS DUE LATENT SOFTWARE DEFECTS 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 potential hazards caused by CCFs of digital technology, in particular within software or software-based logic. 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 modification is consistently applied. This is in addition to clarifying specific areas of guidance such as diversity and testing to eliminate further consideration of CCF hazards. 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 hazards.