U.S. NUCLEAR REGULATORY COMMISSION

# STANDARD REVIEW PLAN

## BRANCH TECHNICAL POSITION 7-19

## GUIDANCE FOR EVALUATION OF DEFENSE IN DEPTH AND DIVERSITY TO ADDRESS COMMON-CAUSE FAILURE DUE TO LATENT DESIGN DEFECTS IN DIGITAL SAFETY SYSTEMS

## REVIEW RESPONSIBILITIES

Primary – Organization responsible for the review of instrumentation and controls (I&C) to ensure the I&C equipment performs the functions credited in the safety analysis

Secondary – Organizations responsible for (1) the review of reactor and containment systems, (2) the review of human factors engineering (HFE), and (3) the review of risk assessments

**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 Power Plants: LWR Edition" (SRP), Section 7.1-T, "Table 7-1 Regulatory Requirements, Acceptance Criteria, and Guidelines for Instrumentation and Control Systems Important to Safety" (table 7-1). This BTP does include the associated year in references to industry standards incorporated by reference into regulations (Institute of Electrical and Electronics

Draft Revision 9—October 2023

Engineers (IEEE) Standard (Std) 279-1968, “Proposed IEEE Criteria for Nuclear Power Plant Protection Systems”; IEEE Std 279-1971, “Criteria for Protection Systems for Nuclear Power Generating Stations”; and IEEE Std 603-1991, “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations”), as well as industry standards that are not endorsed by the agency. Users should consult table 7-1 to ensure that reviews apply the appropriate RGs and endorsed industry standards.

The acceptance criteria provided in this BTP are not limited to performance characteristics of the I&C systems but are instead intended to address plant performance in response to common-cause failures (CCFs) of the I&C systems. As such, the evaluation activities described in this BTP are not intended to be exclusively assigned to I&C technical review staff. For any given project, the activities should be coordinated and distributed among the various technical review disciplines to ensure that the correct area of review and level of expertise are applied to the evaluation effort. For example, a reactor safety system engineer should perform the evaluation of a “best estimate” analysis for each postulated accident (PA) or other event, while the determination of adequate independence in the design of a proposed diverse actuation system would be the responsibility of the I&C technical reviewer.

## A. BACKGROUND

Digital technology offers significant operational and maintenance benefits for I&C systems of nuclear power plants (NPPs). Digital I&C (DI&C) systems consist of both hardware components and logic elements (e.g., software). Hardware components in DI&C systems are susceptible to failures similar to those considered for analog systems. In this guidance, the term “software” refers to software, firmware, and logic developed from software-based development systems (e.g., hardware description language (HDL) programmed devices).

DI&C systems or components may be vulnerable to CCFs due to latent design defects in active hardware components, software, or software-based logic.[1] A CCF occurs when multiple (usually identical) systems or components fail due to a shared cause.[2] Latent design defects in the design of the DI&C system or component can remain undetected. Certain events, unexpected external stresses, or plant conditions can trigger latent design defects within redundant portions (e.g., safety divisions) of a system designed to perform safety functions and thus lead to a systematic failure of the redundant portions.

CCFs can have two different effects: (1) they can cause a loss of the capability to perform a safety function or can initiate a plant transient, or (2) they can initiate the operation of a function without a valid demand or can cause an erroneous (i.e., spurious) system action. The latter is typically referred to as “spurious operation” or “spurious actuation.” CCFs with a loss of safety function are postulated concurrent with an anticipated operational occurrence (AOO), a PA, or normal operations, while spurious operations are postulated as an initiating event.

---

1 Where this BTP refers to “CCF,” it is always referring to CCF due to a latent design defect in active hardware components, software, or software-based logic.

2 CCFs due to latent design defects in DI&C SSCs are similar to but distinguishable from cascading failures due to single random failures. Single failures must be addressed by meeting the criteria described in Title 10 of the *Code of Federal Regulations* (10 CFR) 50.55a(h) (i.e., they are required to address safety design criteria in IEEE Std 279-1971 or IEEE Std 603-1991). Because such failures are likely to occur during the life of the plant, the design basis for the plant needs to consider the analysis of the possible effects (consequences) of such failures.

In accordance with Commission direction in the NRC staff requirements memorandum (SRM) on SECY-93-087, "SECY-93-087—Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," dated July 21, 1993, the NRC staff considers CCFs in DI&C systems to be beyond-design-basis events. The likelihood of occurrence of these failures cannot be predicted through traditional design analysis methods, but their effects and consequences can be addressed through other methods, such as best estimate methods.

DI&C system modifications can interconnect design functions that were previously located in separate or dedicated equipment, and these modifications can therefore introduce new failure mechanisms. Also, DI&C systems can share resources, such as communications, networks, controllers, power supplies, or multifunction display and control stations. The resulting interdependencies of DI&C systems make it more challenging to identify and evaluate potential consequences of a postulated CCF.

Generally, except in a few structures, systems, and components (SSCs) with relatively simple designs, DI&C systems cannot be fully tested, nor can their failure mechanisms be completely known, because their complexity leads to too many potential failure mechanisms. Therefore, DI&C systems may be vulnerable to a CCF if any of the following are present in redundant divisions of the systems: (1) identical system requirements or designs, (2) identical copies of the software or software-based logic, or (3) unidentified dependencies, unintended interactions, and emergent behavior, especially when the DI&C systems are interconnected or use shared resources.

Traditionally, CCF vulnerabilities of DI&C systems or components have been addressed using the principles of diversity and defense in depth (D3). Under these principles, the operation of facility systems is modeled as a series of successive layers of defense (called "echelons of defense"), each of which would need to be defeated for a CCF to result in unacceptable harm to public health and safety. A CCF could affect multiple echelons of defense and redundant divisions, depending upon, for example, the system architecture, extent of interconnections, and type and use of shared resources. NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems," issued December 1994, describes defense in depth for NPPs. For example, section 2.2 of NUREG/CR-6303 identifies the normal reactor control systems, the reactor trip system (RTS), the engineered safety features actuation system, and the reactor monitoring and indication systems as individual echelons of defense. Generally, the design technique of independence (e.g., communication independence) is used to ensure that multiple echelons do not fail concurrently.

An overall DI&C system architecture that maintains the integrity of multiple layers of defense is key to ensuring a system's ability to limit, mitigate, withstand, or cope with the effects of a CCF. Traditional design techniques such as redundancy, independence (e.g., communication independence), and diversity provide the basic framework and structure for maintaining defense in depth. Other design features (or design techniques) can also contribute to overall defense in depth. Such features (or design techniques) include predictable real-time (deterministic) processing; automated self-test provisions; and measures to control access to physical, electronic, and software-based elements that, if tampered with or corrupted, could cause adverse plant consequences. The following documents provide NRC staff guidance for evaluating these features:

- SRP Appendix 7.0-A, “Review Process for Digital Instrumentation and Control Systems,” and BTP 7-21, “Guidance on Digital Computer Real-Time Performance,” provide guidance on real-time deterministic processing.

- Item B.3.1 of table 2 and item C.7 of table 3 in SRP Section 13.6.6, “Cyber Security Plan,” provide guidance on control of access.

- RG 1.152, “Criteria for Programmable Digital Devices in Safety-Related Systems of Nuclear Power Plants,” provides guidance on measures protecting against undesirable acts (e.g., tampering with software code or logic) that can compromise the safety system.

- RG 5.71, “Cybersecurity Programs for Nuclear Power Reactors,” provides guidance on protecting digital computers and communication systems and networks against cyberattacks.

- BTP 7-17, “Guidance on Self-Test and Surveillance Test Provisions,” provides guidance on self-test features.

Over the years, the NRC staff has approved applications that use various design features to address CCF vulnerabilities in DI&C systems. Some of these use multiple design solutions within different parts of a single DI&C system. In reviewing these applications, the NRC staff has evaluated several different solutions that successfully address CCF vulnerabilities. Consequently, the NRC staff recognizes that there may be no single solution that applies to all DI&C systems.

## 1 Regulatory Basis

The regulations listed below may not apply to all applicants. Their applicability depends on the plant-specific licensing basis and any proposed changes to the licensing basis associated with the DI&C system under evaluation:

- For NPPs with construction permits (CPs) issued before January 1, 1971, 10 CFR 50.55a(h) requires protection systems to be consistent with the plant-specific licensing basis or to comply with IEEE Std 603-1991 and the IEEE Std 603-1991 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 protection systems to comply with IEEE Std 279-1968, IEEE Std 279-1971, or IEEE Std 603-1991 and the correction sheet dated January 30, 1995.

- For applications for CPs, operating licenses (OLs), combined licenses (COLs), standard design approvals (SDAs), or design certifications (DCs) filed after May 13, 1999, 10 CFR 50.55a(h) requires compliance with IEEE Std 603-1991 and the correction sheet dated January 30, 1995.

- General Design Criterion (GDC) 22, “Protection system independence,” of Appendix A, “General Design Criteria for Nuclear Power Plants,” to 10 CFR Part 50, “Domestic Licensing of Production and Utilization Facilities,” states the following:

> The protection system shall be designed to assure 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, or shall be demonstrated to be acceptable on some other defined basis. 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 24, "Separation of protection and control systems," of Appendix A to 10 CFR Part 50 states in part that "interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired."

- GDC 25, "Protection system requirements for reactivity control malfunctions," of Appendix A to 10 CFR Part 50 states, "The protection system shall be designed to assure that specified acceptable fuel design limits are not exceeded for any single malfunction of the reactivity control systems, such as accidental withdrawal (not ejection or dropout) of control rods."

- GDC 26, "Reactivity control system redundancy and capability," of Appendix A to 10 CFR Part 50 states the following:

  > Two independent reactivity control systems of different design principles shall be provided. One of the systems shall use control rods, preferably including a positive means for inserting the rods, and shall be capable of reliably controlling reactivity changes to assure that under conditions of normal operation, including anticipated operational occurrences, and with appropriate margin for malfunctions such as stuck rods, specified acceptable fuel design limits are not exceeded. The second reactivity control system shall be capable of reliably controlling the rate of reactivity changes resulting from planned, normal power changes (including xenon burnout) to assure acceptable fuel design limits are not exceeded. One of the systems shall be capable of holding the reactor core subcritical under cold conditions.

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

- The regulations in 10 CFR Part 100, "Reactor Site Criteria," Subpart A, "Evaluation Factors for Stationary Power Reactor Site Applications Before January 10, 1997 and for Testing Reactors," apply to holders of and applicants for OLs whose CPs were issued before January 10, 1997, and required the CP applicant to assume a fission product release from the core for use in deriving an exclusion area, a low-population zone, and a population center distance. The dose criteria in 10 CFR 100.11(a) are commonly referred to as "site dose guideline values" and provide reference values for site evaluation, which can also be used as acceptance criteria for evaluating the adequacy of DI&C design by considering the consequences of a CCF concurrent with a design-basis event (DBE).

- In 10 CFR 50.67, “Accident source term,” the NRC provides dose guideline values for analysis of the acceptability of a fission product release from a currently operating NPP as an alternative source term.

- The regulations in 10 CFR 50.69, “Risk-informed categorization and treatment of structures, systems and components for nuclear power reactors,” allow a licensee or applicant to voluntarily comply with the requirements of that section as an alternative to the requirements in 10 CFR 50.69(b) by implementing a risk-informed categorization and treatment of the SSCs of its nuclear power reactor.

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

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

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

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

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

## 2 Relevant Guidance

The following documents provide useful guidance for the evaluation of possible CCFs in digital safety system designs:

- NUREG/CR-6303 summarizes several D3 analyses performed after 1990. It presents a method for analyzing proposed DI&C systems to identify vulnerabilities to common-mode failures[3] and to confirm that the design incorporates adequate D3 strategies to address them. This analysis method postulates common-mode failures that could occur within digital reactor protection systems and determines what portions of a design need additional D3 measures to address such failures.

- NUREG/CR-7007, “Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems,” issued February 2010, provides diversity strategies to mitigate CCF vulnerabilities in a safety-related system for which a D3 assessment has shown a need for greater diversity. NUREG/CR-7007 identifies and develops a baseline set of diversity criteria that may be appropriate for addressing potential vulnerabilities to CCFs. 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.

[3] Note that while these documents use the term “common-mode failure,” this BTP uses the term “common-cause failure” because it better characterizes this type of failure.

- SECY-93-087, dated April 2, 1993, item II.Q, as clarified by SRM-SECY-93-087, item 18, describes the NRC position on defense against potential common-mode failures in DI&C systems.

- SECY-18-0090, "Plan for Addressing Potential Common Cause Failure in Digital Instrumentation and Controls," dated September 12, 2018, describes the NRC staff's plan to clarify the guidance for evaluating and addressing potential CCFs of DI&C systems.

- SECY-22-0076, "Expansion of Current Policy on Potential Common-Cause Failures in Digital Instrumentation and Control Systems," dated August 10, 2022, describes the NRC staff's proposal to clarify, further risk-inform, and expand the NRC's policy for evaluating and addressing potential CCFs of DI&C systems. Specifically, the SECY requested that the Commission expand the current policy to allow the use of risk-informed approaches to demonstrate the appropriate level of defense-in-depth, including not providing any diverse automatic actuation of safety functions, and that this expanded policy would apply to all NPP types.

- The supplement to SECY-22-0076, dated January 23, 2023, clarifies the NRC staff's proposal in SECY-22-0076.

- SRM-SECY-22-0076, dated May 25, 2023, approved the NRC staff's recommendation in SECY-22-0076, with edits, and provided directions to the NRC staff. Specifically, the Commission directed that the proposed revision to the CCF policy (as amended by the SRM) be applied independent of the licensing pathway.

- SRM-SECY-10-0121, dated March 2, 2011, disapproved the staff's recommendation to modify risk guidance for new reactors described in SECY-10-0121 and reaffirmed that the existing safety goals, safety performance expectations, subsidiary risk goals and associated risk guidance (such as the Commission's 2008 Advanced Reactor Policy Statement and Regulatory Guide 1.174), key principles and quantitative metrics for implementing risk-informed decision-making, are sufficient for new plants.

- Generic Letter (GL) 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. GL 85-06 describes methods that may be used to establish quality assurance measures for such equipment that is credited for providing the diverse means to mitigate potential CCFs.

- RG 1.62, "Manual Initiation of Protective Actions," describes a method that the NRC staff considers acceptable for use in complying with the NRC's regulations concerning the means for manual initiation of protective actions provided (1) by otherwise automatically initiated safety systems or (2) as a method diverse from automatic initiation.

- 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.

- RG 1.152, “Criteria for Programmable Digital Devices in Safety-Related Systems of Nuclear Power Plants,” provides guidance on measures to ensure communication independence and control of access. For an application that describes cybersecurity design features intended to address cybersecurity vulnerabilities, the NRC staff’s review of these features is limited to ensuring that they do not adversely affect or degrade the safety-related system’s reliability or its capability to perform its safety functions. If licensees and applicants consider the cybersecurity design features, measures should be included to ensure that safety-related I&C systems do not present an electronic path that could enable unauthorized access to the plant’s safety-related system (e.g., the use of a hardware-based unidirectional device is one approach the NRC staff would consider acceptable for implementing such measures).

- RG 1.174, “An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis,” describes an approach that is acceptable to the NRC staff for developing risk-informed applications for a licensing basis change that considers engineering issues and applies risk insights.

- RG 1.200, “Acceptability of Probabilistic Risk Assessment Results for Risk-Informed Activities,” describes one approach acceptable to the NRC staff for determining whether a base probabilistic risk assessment (PRA), in total or in the portions that are used to support an application, is sufficient to provide confidence in the results, such that the PRA can be used in regulatory decision-making for light-water reactors.

- SRP Section 7.1-T, “Table 7-1 Regulatory Requirements, Acceptance Criteria, and Guidelines for Instrumentation and Control Systems Important to Safety,” provides the revision numbers of RGs and the years of endorsed industry standards referenced in this BTP.

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

- 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 the potential for CCFs.

- SRP Chapter 18, “Human Factors Engineering,” provides a methodology for evaluating manual actions credited with the accomplishment of functions important to safety.

- SRP Section 19.2, “Review of Risk Information Used to Support Permanent Plant-Specific Changes to the Licensing Basis: General Guidance,” provides review guidance for probabilistic risk assessments used by licensees or applicants to support licensing applications.

Scope

The guidance in this BTP is intended for the NRC staff reviews of I&C safety systems proposed (1) in requests for license amendments as modifications to licensed NPPs or (2) in applications for CPs, OLs, COLs, DCs, SDAs, and MLs. This BTP does not apply to proposed modifications performed under the change process in 10 CFR 50.59, “Changes, tests and experiments.” This BTP provides review guidance to the I&C technical review staff for evaluating whether an

applicant's proposed DI&C design complies with the functional goals established by (1) the applicable safety analysis, (2) principles of risk-informed decision-making, as applicable, (3) specific regulations, and (4) Commission policy.

This BTP does not cover review criteria for single random failures and cascading failures from single random failures in shared resources (i.e., not due to latent design defects in DI&C SSCs). The reviewer can find guidance for addressing single failures in systems credited to perform safety functions in RG 1.53, "Application of the Single-Failure Criterion to Safety Systems." SRP section 7.7 provides guidance for analyzing postulated failures in systems that are not safety related.

Purpose

This BTP provides the NRC staff with guidance for evaluating an applicant's assessment of the adequacy of D3 for a proposed DI&C system. The applicant performs this D3 assessment to identify and address potential CCFs in a proposed DI&C system and to evaluate the effects of any unprevented CCFs on plant safety.

This BTP also provides guidance for review of the following:

- the appropriateness of an applicant's chosen methods for performing a D3 assessment, including any categorization of proposed DI&C SSCs based on the safety significance of the functions they perform

- proposed design attributes—such as the use of diverse equipment, testing, or alternative approaches in the design of a system or component—that may eliminate a potential CCF from further consideration[4]

- an applicant's use of diverse equipment (external to the DI&C system), including manual controls and displays, to mitigate a potential CCF, as well as other measures to ensure conformance with the NRC's position on addressing CCFs in DI&C systems as specified in SRM-SECY-93-087, SECY-18-0090, and SRM-SECY-22-0076

This BTP also addresses review of the applicant's assessment of vulnerabilities to a CCF that can cause a spurious operation. It provides the NRC staff with guidance for evaluating applicant analyses of a DI&C system's ability to withstand or cope with CCFs resulting in spurious operations.

## B. BRANCH TECHNICAL POSITION

1. Introduction

The overall objective of this BTP is to provide criteria for the NRC staff's evaluation of the acceptability of the applicant's D3 assessment of the effects of DI&C system CCFs.

For this evaluation, the reviewer should confirm that the application includes the following:

[4] Section B.3.1 of this BTP describes how a potential CCF can be eliminated from further consideration.

- a description of the overall defense-in-depth posture of plant control and protection systems adequate to protect the plant from the effects of CCFs if they were to occur
- identification and documentation of vulnerabilities to CCF
- a documented basis for any safety-significance determinations used in the application
- a failure analysis for any SSCs excluded from a D3 assessment
- a description of any D3 assessment, including the following:
  - an evaluation of vulnerabilities to a CCF, and any means (e.g., design features or design techniques) used to eliminate the potential CCF from further consideration
  - identification and evaluation for effectiveness of any design features, design techniques, prevention measures, or mitigation measures, other than diversity, that are credited in the assessment
  - identification and evaluation for effectiveness of diverse measures credited by the applicant to mitigate potential consequences from CCF vulnerabilities
  - an assessment of the effects associated with residual CCF vulnerabilities that have not been either eliminated from further consideration or mitigated in some manner, and whether the assessment demonstrates that (1) the consequences of the residual CCF remain acceptable or (2) the residual CCF is not risk significant

The reviewer should consider whether the applicant's assessment has properly identified and addressed CCFs and whether the applicant has incorporated appropriate means to limit, mitigate, or withstand or cope with (i.e., accept the consequences of) possible CCFs and sources of CCF vulnerability that can result in spurious operations. Alternatively, if the application includes a risk-informed approach, the reviewer should consider whether the assessment demonstrates that the residual CCF is not risk significant.

## 1.1 Common-Cause Failure Position and Discussion

The foundation of BTP 7-19 is the NRC position on D3 from SRM-SECY-93-087 as expanded by SRM-SECY-22-0076, which predominately consists of the four points below:

1. The applicant must assess the defense in-depth and diversity of the facility incorporating the proposed digital I&C system to demonstrate that vulnerabilities to digital CCFs have been adequately identified and addressed.

   The defense-in-depth and diversity assessment must be commensurate with the risk significance of the proposed digital I&C system.

2. In performing the defense-in-depth and diversity assessment, the applicant must analyze each postulated CCF using either best-estimate methods or a risk-informed approach or both.

When using best-estimate methods, the applicant must demonstrate adequate defense-in-depth and diversity within the facility's design for each event evaluated in the accident analysis section of the safety analysis report.

When using a risk-informed approach, the applicant must include an evaluation of the approach against the Commission's policy and guidance, including any applicable regulations, for risk-informed decision-making. The NRC staff will review applications that use risk-informed approaches for consistency with established NRC policy and guidance on risk-informed decision-making (e.g., Regulatory Guide (RG) 1.174, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis," RG 1.233, "Guidance for a Technology-Inclusive, Risk-Informed, and Performance-Based Methodology to Inform the Licensing Basis and Content of Applications for Licenses, Certifications, and Approvals for Non-Light-Water Reactors").

3. The defense-in-depth and diversity assessment must demonstrate that a postulated CCF can be reasonably prevented or mitigated or is not risk significant. The applicant must demonstrate the adequacy of any design techniques, prevention measures, or mitigation measures, other than diversity, that are credited in the assessment. The level of technical justification demonstrating the adequacy of these techniques or measures, other than diversity, to address potential CCFs must be commensurate with the risk significance of each postulated CCF.

   A diverse means that performs either the same function or a different function is acceptable to address a postulated CCF, provided that the assessment includes a documented basis showing that the diverse means is unlikely to be subject to the same CCF. The diverse means may be performed by a system that is not safety-related if the system is of sufficient quality to reliably perform the necessary function under the associated event conditions. Either automatic or manual actuation within an acceptable timeframe is an acceptable means of diverse actuation.

   If a postulated CCF is risk significant and the assessment does not demonstrate the adequacy of other design techniques, prevention measures, or mitigation measures, then a diverse means must be provided.

4. Main control room displays and controls that are independent and diverse from the proposed digital I&C system (i.e., unlikely to be subject to the same CCF) must be provided for manual, system-level actuation of risk-informed critical safety functions and monitoring of parameters that support the safety functions. These main control room displays and controls may be used to address point 3, above. The applicant may alternatively propose a different approach to this point in the policy if the plant design has a commensurate level of safety.

The following BTP sections apply to the evaluation of an application against these four points:

- Point 1—determine the need for a detailed D3 assessment
  - section B.2.1 for making a safety-significance determination
  - section B.2.2 for using the safety significance to determine whether a detailed D3 assessment is necessary
  - section B.3.1 for determining whether a CCF can be eliminated from further consideration
    - section B.3.1.1 for the use of diversity within the DI&C system
    - section B.3.1.2 for the use of testing
    - section B.3.1.3 for the use of methods other than diversity and testing
    - section B.3.1.4 for the use of a qualitative assessment and failure analysis
- Point 2—perform a detailed D3 assessment to address each CCF
  - section B.3.2 for the use of best estimate methods
  - section B.3.4 for the use of risk-informed approaches
    - section B.3.4.1 for determining consistency with NRC policy and guidance on risk-informed decision-making
    - section B.3.4.2 for modeling a CCF
- Point 3—address, mitigate, or accept the consequences of a CCF
  - section B.3.2 for crediting diverse means to mitigate the impact of a CCF
    - section B.3.2.1 for crediting existing systems
    - section B.3.2.2 for crediting manual operator action
    - section B.3.2.3 for crediting a new diverse system
  - section B.3.3 for determining whether the consequences of a CCF may be acceptable
  - section B.3.4 for design techniques or mitigating measures other than diversity
    - section B.3.4.3 for determining the risk significance of the CCF
    - section B.3.4.4 for determining the appropriate means to address the CCF
- Point 4—provide independent and diverse displays and manual controls

– section B.4 for manual system-level actuation and indication of critical safety functions to address Point 4

Figures 7-19-1, 7-19-2, 7-19-3, and 7-19-4 at the end of this document provide a visual aid to the reviewers when reviewing an application against the four points.

The guiding principles in SECY-18-0090 clarify that the D3 assessment described in Point 1 should be commensurate with the safety significance of the proposed DI&C system.

As modified in SRM-SECY-22-0076, Point 1 allows for consideration of the risk significance of the DI&C system and the CCF. Specifically, Point 1 calls for the D3 assessment to be commensurate with the risk significance of the proposed DI&C system.

Point 2 uses the term "best estimate methods," which is generally understood to refer to methods that use realistic assumptions, i.e., the initial plant conditions corresponding to the onset of the event being analyzed. Point 2 also includes acceptance criteria for "best estimate methods" that are less conservative than the acceptance criteria defined in the updated final safety analysis report (FSAR) for the applicable limiting events within the design basis. Initial plant event conditions include, but are not limited to, the following:

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

SECY-18-0090 clarifies that, in addition to the "best estimate" methods using realistic assumptions identified in Point 2, the "best estimate" D3 assessment can be performed using a design-basis analysis.[5] The key distinction is that a design-basis analysis uses conservative assumptions. Reviewers should consider whether each event analyzed in the accident analysis is evaluated in the "best estimate" 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.

Point 3 refers to the risk significance of CCFs, whereas Point 1 refers to the risk significance of the proposed DI&C system. Section B.3.4 discusses these concepts. Point 3 calls for an applicant to demonstrate that a postulated CCF be reasonably prevented or mitigated or that the CCF is not risk significant. An applicant can do this by demonstrating the adequacy of the design techniques and prevention and mitigation measures credited in the D3 assessment. If the D3 assessment demonstrates that a CCF can be reasonably prevented or mitigated by other means (e.g., using other installed systems) or that the CCF is not risk significant, then a diverse means that performs the same or a different function may not be needed.

When a diverse means is provided, Point 3 allows for the diverse means to be comprised of safety-related equipment or equipment that is not safety related, together with a documented

[5] Although SRM-SECY-22-0076 stated that the best estimate methods must be used, the NRC staff understands that design-basis analyses are conservative and could also be an acceptable analysis method. The NRC staff understands the SRM to mean that applicants are not required or obligated to use design-basis analysis methods.

basis that this equipment is of sufficient quality and is unlikely to be subject to the same CCF. Methods for demonstrating sufficient quality include quality controls or measures developed in accordance with GL 85-06 and alternative treatment similar to that required for RISC-2 SSCs in 10 CFR 50.69(d)(1), if applicable. The diverse means may already exist in the facility or may be installed in connection with the DI&C modification. For example, an ATWS system may be credited as the diverse means of tripping the reactor, provided it is not vulnerable to the same CCF that could disable the safety function.

If a diverse means is part of a safety-related system, it is then subject to the divisional independence requirements in IEEE Std 603-1991, clause 5.6.1, which is incorporated by reference into 10 CFR 50.55a, "Codes and standards." If the diverse means is equipment that is not safety related, then the requirements in IEEE Std 603-1991, clause 5.6.3, for separation and independence between safety-related systems and other systems would apply.

The displays and controls credited for Point 4 must provide for effective manual control of critical safety functions. Point 4 clarifies that these main control room (MCR) displays and controls may be addressed in the same assessment as the first three points (i.e., does not require a separate analysis beyond what is called for in Points 1–3 of the policy). Point 4 is risk-informed because it focuses only on those most important safety functions to be accomplished or maintained to prevent a direct and immediate threat to public health and safety (see Section B.1.2), because the diverse displays and manual controls do not have to be safety related or hardwired, and because the applicant may alternatively propose a different approach to this point in the policy, if the plant design has a commensurate level of safety.

### 1.2 Critical Safety Functions

Critical safety functions are those most important safety functions to be accomplished or maintained to prevent a direct and immediate threat to public health and safety.[6] The NRC staff's proposal in SECY-93-087, as amended and approved by SRM-SECY-93-087, identified the following examples of critical safety functions to be managed from the MCR in accordance with Point 4:

- reactivity control
- core heat removal
- reactor coolant inventory
- containment isolation
- containment integrity

[6] The use of the term "critical safety functions" goes back to American National Standards Institute/American Nuclear Society-4.5-1980, "Criteria for Accident Monitoring Functions in Light-Water-Cooled Reactors," and IEEE Std 497-1981, "IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations." The most important safety functions may not always be called "critical safety functions." For example, while IEEE Std 497-2002, which was conditionally endorsed by RG 1.97, Revision 4, "Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants," issued June 2006, uses the term "critical safety function," IEEE Std 497-2016, which was conditionally endorsed by RG 1.97, Revision 5, issued April 2019, uses the term "safety function" when referring to the same critical safety functions listed in IEEE Std 497-2002. Another example is the use of the term "fundamental safety functions" in NUREG-2246, "Fuel Qualification for Advanced Reactors," issued March 2022, which refers to the 2018 International Atomic Energy Agency safety glossary definition for the term.

The critical safety functions listed in SECY-93-087 and SECY-22-0076 are representative of operating light-water reactors. Other types of reactors may have different critical safety functions. The identification of these critical safety functions is a plant-specific activity performed by applicants that is based on the reactor design safety analysis and may be risk-informed. Risk-informed approaches may be used to identify the most important safety functions to be accomplished or maintained to prevent a direct and immediate threat to public health and safety.

Section 4 of this BTP provides acceptance criteria for the implementation of diverse and independent displays and manual controls for actuation of these critical safety functions.

## 2. Safety Significance and Effects of Failure

Principle 3 of SECY-18-0090 explained that the D3 assessment "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." Point 1 of the revised policy states that the D3 assessment must be commensurate with the risk significance of the digital I&C system, as described further below. Furthermore, Point 3 of the revised policy states that the level of technical justification demonstrating the adequacy of design techniques, prevention measures, or mitigation measures, other than diversity, credited in the assessment to address potential CCFs must be commensurate with the risk significance of each postulated CCF.

Specifically, this section provides guidance for reviewing (1) the relative safety significance of the functions performed by an SSC and (2) an application that does not include a detailed D3 assessment for an SSC of lowest safety significance based on the potential effects of the SSC's failure.

### 2.1 Safety-Significance Determination

For the purposes of this BTP, a safety-significant function is one whose degradation or loss could have a significant adverse effect on defense in depth, safety margin, or risk. For example, because immediate responses are needed for certain adverse reactor conditions, the RTS and engineered safety features actuation system are generally deemed more critical than those systems that perform auxiliary safety functions that are not directly credited in the accident analysis. Consequently, a CCF assessment for an RTS should, generally, be more rigorous than one for a safety-related MCR heating, ventilation, and air conditioning (HVAC) chiller. While the HVAC chiller is a safety-related system, maintaining a certain temperature and humidity in the MCR to allow equipment and personnel to operate properly, a failure of this system is not as significant as an RTS failure because personnel have operating procedures or diverse means to control MCR temperature and humidity and can shut down the plant for this purpose if necessary. Therefore, the reviewer should evaluate the applicant's safety-significance determination for the SSC subject to the D3 assessment.

The reviewer should consider whether the applicant used risk insights from site-specific PRAs, if available, to support its determination. The reviewer should confirm that the application documents the basis for the safety-significance determination, including any use of risk insights. The reviewer should also determine whether the use of risk insights is reasonable.

System Interconnectivity

System interconnectivity can introduce additional dependencies and therefore CCF vulnerabilities. If there is interconnectivity, the system should be assessed using the methods appropriate for the SSC of most safety significance that is interconnected. The reviewer should consider whether the applicant included a clear description of the proposed DI&C system or component that identifies (1) shared resources, (2) interconnection with other systems, and (3) whether a modification could reduce the redundancy, diversity, separation, or independence of systems described in the facility's FSAR. Reductions in independence, separation, diversity, or redundancy can adversely affect the defense in depth of a plant. For data-communication interconnectivity, the reviewer should verify that such interconnectivity would not adversely affect or degrade the safety-related system's reliability or its capability to perform its safety functions. RG 1.152 provides, in part, guidance for data communication independence, control of access, and prioritization of control and protection systems sharing components.

The reviewer should also determine whether the assessment of the most safety-significant SSCs considers the vulnerability to CCF resulting from failures within the interconnected system and the consequences of a CCF that could affect the proper operations of the interconnected systems. If the reactor trip or engineered safety feature initiation signal in such a system reaches the final actuation device only through the equipment that performs control functions, then the reviewer should determine whether all the SSCs in that pathway have been assigned to the SSC category of most safety significance.

Acceptance Criteria for Safety-Significance Determinations

Safety-significance determination categories should reasonably conform to the criteria below. If the applicant uses risk insights (e.g., from a site-specific PRA) to demonstrate that an SSC is less safety significant than these criteria would indicate, the NRC staff should review these on a case-by-case basis. The following acceptance criteria apply:

a. high safety significance: safety-related SSCs that perform safety-significant functions

SSCs in this category have one or more of the following characteristics:

- They are credited in the FSAR to perform design functions that contribute significantly to plant safety.
- They are relied upon to initiate and complete control actions essential to maintaining plant parameters within acceptable limits established for a DBE or to maintaining the plant in a safe state after it has reached safe shutdown.
- Their failure could directly lead to accident conditions that may have unacceptable consequences (e.g., exceeding dose guidelines) if no other automatic systems are available to provide the safety function or no preplanned manual operator actions have been validated to provide the safety function.

b. lower safety significance: safety-related SSCs that do not perform safety-significant functions, and SSCs that are not safety related that do perform safety-significant functions

SSCs in this category have one or more of the following characteristics:

- They provide an auxiliary or indirect function in the achievement or maintenance of a safety-related function.
- They perform a design function that is not safety related that contributes significantly to plant safety.
- They are capable of directly changing the reactivity or power level of the reactor, and their failure could initiate an accident sequence or could adversely affect the integrity of a safety barrier (i.e., fuel cladding, reactor vessel, or containment).
- They are credited in the FSAR for meeting diversity requirements.

c. lowest safety significance: SSCs that are not safety related that do not perform safety-significant functions

SSCs in this category have one or more of the following characteristics:

- They perform functions that are not considered significant contributors to plant safety.
- They have no direct effect on the reactivity or power level of the reactor and do not affect the integrity of a safety barrier (i.e., fuel cladding, reactor vessel, or containment).

2.2 Using Safety Significance to Determine When a Detailed Diversity and Defense-in-Depth Assessment Is Necessary

A detailed D3 assessment is necessary for all systems determined to be of high safety significance. As stated in SECY-18-0090, a D3 assessment demonstrates "that failures due to software or failures propagated through connectivity cannot result in a failure to perform safety functions or adverse plant conditions that cannot be reasonably mitigated." Therefore, in accordance with Principle 3 in SECY-18-0090, a D3 assessment "may not be necessary for some low-safety-significance I&C systems" if the application demonstrates that the failure of the SSC "would not adversely affect a safety function or place a plant in a condition that cannot be reasonably mitigated."

Acceptance Criteria for Elimination of Further Consideration of Diversity and Defense in Depth

If the application meets the acceptance criteria identified below, the reviewer should conclude that a detailed D3 assessment is not necessary because a failure analysis demonstrates that failure of the specified SSC cannot adversely affect a safety function or place the plant in a condition that cannot reasonably be mitigated. The acceptance criteria are as follows:

- The SSC has the characteristics listed in item (c) of section B.2.1 above or documented risk insights demonstrate that its level of safety significance is similar to that of SSCs with those characteristics.
- The SSC is not interconnected with a more safety-significant SSC.

- The application includes an analysis of a postulated failure of the SSC to perform its design functions and evaluates the effects of that failure, including potential spurious operations.

- The failure does not adversely affect a safety function or place the plant in a condition that cannot reasonably be mitigated.

3. Detailed Diversity and Defense-in-Depth Assessment

A D3 assessment is a systematic approach used to analyze a proposed DI&C system for CCFs that can occur concurrently within a redundant design, for example, within two or more independent divisions. These CCFs could cause the DI&C system to fail to perform its intended safety function or could lead to spurious operations. The reviewer should evaluate whether the D3 assessment considers the entire plant performance characteristics in response to CCF. CCFs for DI&C safety systems of both high and lower safety significance, and SSCs of lowest safety significance that need a detailed D3 assessment, should be evaluated and addressed by considering, as a minimum, the functional partitioning within the DI&C architecture, and whether the CCF could originate in shared resources or could adversely impact any interconnected portions of the DI&C system.

Reviewers should determine whether the applicant's D3 assessment is adequate to protect against CCFs that are either (1) identified through design analysis or (2) postulated as design defects that are not identifiable through design analysis. The reviewer should also consider whether the D3 assessment includes an analysis of the effects of CCFs to verify that these effects are bounded by the acceptance criteria defined in the FSAR or in the license amendment request (LAR) for the limiting events applicable to the proposed DI&C system or component.

A D3 assessment should include the information necessary for the NRC staff to perform its review. When evaluating a D3 assessment, the reviewer should do the following:

- Confirm that a D3 assessment was performed for the proposed system or component to determine whether CCF vulnerabilities have been adequately addressed.

- Evaluate whether the D3 assessment indicates that CCF vulnerabilities have been adequately addressed.

- Evaluate whether the D3 assessment indicates that CCF vulnerabilities that might result in spurious operations have been adequately addressed.

- Confirm that the potential consequences of any residual CCF vulnerabilities not previously addressed have been evaluated and fall within the limiting plant design-basis consequences.

General Approach

The reviewer should consider whether the D3 assessment is adequate to identify and defend against CCF vulnerabilities. Acceptable methods for an applicant to use to address or defend against vulnerabilities include, but are not limited to, the following:

- The applicant eliminated CCF vulnerabilities from further consideration through any of the methods below, either alone or in combination:
  - using diversity within the DI&C system or component (section B.3.1.1)
  - using testing (section B.3.1.2)
  - using alternative approaches (section B.3.1.3)
  - for SSCs of lower or lowest safety significance, using a qualitative assessment and failure analysis (section B.3.1.4)
- The applicant mitigated consequences of CCF vulnerabilities using one or more of the measures in section B.3.2.
- The applicant analyzed consequences of CCF vulnerabilities and found them to remain within the acceptance criteria defined in the FSAR or the LAR for the limiting events applicable to the proposed DI&C (section B.3.3)
- The applicant assessed the risk of CCF vulnerabilities using a risk-informed approach and applied design techniques, prevention measures, or mitigation measures commensurate with the risk significance of the postulated CCF (section B.3.4).

If the applicant used multiple strategies to address CCF vulnerabilities in different portions of a system, then the reviewer should evaluate the applicant's analysis of the CCF vulnerabilities in each portion and identify how each method was applied. For example, in one portion of the system, the applicant might eliminate a CCF from further consideration, while in another portion, the applicant might mitigate the CCF vulnerability using diverse I&C systems.

Spurious Operation as a Result of Common-Cause Failure

The evaluation of potential spurious operations is an important part of the overall D3 assessment for a proposed DI&C system to ensure that spurious operations do not lead to events with unacceptable consequences.

Although a spurious operation is not always anticipated, it can be detected because this type of failure is normally self-announcing through instrumentation on the actuated system. However, in some circumstances, a spurious operation may not occur until a particular signal or set of signals is present. In these cases, rather than occurring immediately upon system startup, the spurious operation would occur only under certain plant conditions. Such a spurious operation is still self-announcing (by the actuated system), even if failure did not occur on initial test or startup.

Because of the potential consequences of a spurious operation, a system's failure to actuate might not be the most limiting failure. This is especially true in view of the time needed to identify and respond to conditions resulting from spurious operation in DI&C systems. In some cases, a failure to trip might be less limiting than a partial actuation. For example, a partial actuation of an emergency core cooling system (i.e., spurious operation of a single division), together with a false indication of a successful actuation, may take an operator longer to evaluate and correct than a total failure to send any actuation signal would. Therefore, the

reviewer should consider the possibilities of both partial actuation and total failure to actuate, together with false indications, stemming from a CCF.

*Sources of Spurious Operation*

Spurious operations originating from CCFs due to latent design defects are considered beyond-design-basis events and are within the scope of this BTP.[7] As stated in the background section of this BTP, CCFs should be evaluated in a manner consistent with SRM-SECY-22-0076. Therefore, the reviewer may apply the methodologies described in this BTP when evaluating spurious operations resulting from CCFs.

*Spurious Operation and Interconnected Systems*

As stated in the background section of this BTP, the interconnection of design functions in a DI&C system makes it challenging to identify CCF vulnerabilities and evaluate their potential consequences. System interconnectivities, including shared resources, may reduce a plant's overall defense in depth (e.g., by reducing independence).

When evaluating interconnected systems, the reviewer should focus primarily on SSCs that are not safety related and that are interconnected with safety-related SSCs. This is because safety-related SSCs have particular regulatory requirements (e.g., for independence and quality) that separately address CCF vulnerabilities in interconnected systems. A secondary focus should be on interconnection of SSCs that can directly or indirectly affect reactivity. In some cases, a system may be susceptible to failures not analyzed in the design bases. The reviewer should consider whether a CCF of an interconnected DI&C system or platform (e.g., a single platform controlling multiple system functions) could result in spurious operation that would have unacceptable consequences. The reviewer should also consider the level of interconnection between safety and other systems as a potential vulnerability to be addressed in the application.[8]

*The NRC Staff's Evaluation of Spurious Operation*

The reviewer should consider whether the D3 assessment addresses spurious operation resulting from CCF along with loss of function resulting from CCF. One important distinction between these two events is that, unlike loss of function, spurious operation is considered an initiating event only, that is, without a concurrent DBE for purposes of this assessment.

## 3.1 Means to Eliminate the Potential for Common-Cause Failure from Further Consideration

In a D3 assessment, the following methods can be used to eliminate a potential CCF from further consideration: (1) demonstration of adequate diversity within the DI&C system or component, (2) testing, and (3) alternative approaches within the application. In addition, for SSCs with lower or lowest safety significance, a qualitative assessment and failure analysis showing that the likelihood of failure is sufficiently low can be used to eliminate a CCF from

---

7 Spurious operations addressed "within the design basis" include spurious operations resulting from single failures (including cascading effects) or single malfunctions. Consistent with regulatory requirements such as those of GDC 25 or those incorporated by reference in 10 CFR 50.55a(h) (namely, IEEE Std 279-1971 or IEEE Std 603-1991), spurious operations resulting from single failures and single malfunctions are expected during the lifetime of the plant and are addressed as part of the design basis.

8 See IEEE Std 603-1991.

further consideration. The reviewer should determine whether the application demonstrates that the use of these methods, alone or in any combination, meets the criteria in this BTP to eliminate the potential CCF from further consideration.

Even if the applicant does not eliminate all CCF vulnerabilities from further consideration using these methods, the reviewer should consider whether there is any portion of the SSC for which the applicant has sufficiently reduced the likelihood of a CCF such that further evaluation is unnecessary for that portion of the SSC.

Each of the following sections discuss one acceptable method to address CCF.

### 3.1.1 Use of Diversity within the Digital Instrumentation and Control System or Component to Eliminate a Potential Common-Cause Failure from Further Consideration

Diversity within a DI&C system or component constitutes the use of different techniques, schemes, features, or additions to eliminate a CCF from further consideration. If diversity is used, each portion of the system or component has different potential latent design defects, so that a failure in one portion will not result in a failure in other portions. Diversity can be implemented in various ways, such as the use of different technologies, algorithms, or logics; sensing devices; or actuation devices. However, diversity needs to be paired with independence from any SSC performing the same function within the digital control system; otherwise, the diverse means could be susceptible to the same CCF.

The reviewer should determine whether the proposed system contains sufficient diversity to perform the safety function, including diversity within each safety division or among redundant safety divisions of a system. If so, then the potential CCF can be eliminated from further consideration. Section 2.6 of NUREG/CR-6303 identifies 6 diversity attributes and 25 related diversity criteria that the reviewer can use to determine whether the system includes adequate diversity. Also, NUREG/CR-7007 identifies and develops a baseline set of diversity criteria that may characterize appropriate diversity strategies for mitigating CCF vulnerabilities. However, the quantification methodology described in NUREG/CR-7007 should not be used as the sole basis for justifying adequate diversity.

Acceptance Criteria for Use of Diversity Within Digital Instrumentation and Controls

If the acceptance criteria below are met, the reviewer should conclude that the application provides adequate information on the use of diversity within the system or component to eliminate CCFs from further consideration. The acceptance criteria are as follows:

a. Each safety function to be achieved by the proposed design is shown to be independently achievable by each diverse portion in the system or component. Diversity between the different portions of the system or component is sufficient to account for potential spurious operation.

b. The different portions of the system or component are sufficiently diverse to perform the safety function without relying on the performance of common components, and the SSCs and software of the different portions are not vulnerable to the same CCFs.

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, whose failure could affect both or all portions. Also, the diverse portions of the system or

component do not share engineering or maintenance tools whose failure could affect both or all portions.

d. Each diverse portion used to perform the credited safety functions is shown to be reliable and available in the plant conditions during which the associated event needs to be prevented or mitigated.

e. Periodic surveillance criteria are used to verify the continuing functionality of each diverse portion.

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

CCF vulnerabilities in DI&C systems or components have two general causes: (1) errors introduced by the system hardware or software design and (2) errors or defects introduced during the development of the software, hardware, or software-based logic. When designing an I&C system, the applicant might use a robust (high-quality) development process, in conjunction with thorough system analysis (e.g., failure modes and effects analysis, system theoretic process analysis), to correct many potential design errors in the requirements or specifications for both analog and digital equipment.

Thorough testing can help to identify latent design defects in DI&C systems, provided the design is simple enough to allow such testing. Testing can be used to uncover latent design defects for correction in the design process and to demonstrate that any identified latent design defects have been corrected. The reviewer should determine whether testing of the proposed DI&C system or component shows that all latent design defects have been identified and corrected, so that the system or component will function as specified under the AOOs. If so, the CCF can be eliminated from further consideration.

The applicant may use various testing methods, which the reviewer should consider on a case-by-case basis. In each case, the reviewer should consider whether the technical basis for these testing methods is acceptable.

Acceptance Criteria for Use of Testing

If the acceptance criteria below are met, the reviewer should conclude that the application provides sufficient information on the test results and testing methodology for a device or component to eliminate a potential CCF from further consideration. The acceptance criteria are as follows:

a. Testing covers the expected performance of the proposed I&C system in each of its functional modes of operation and for all transitions between modes. For this purpose, testing may include the following:

- every possible combination of inputs, including every possible sequence of inputs (if the system has unused inputs, and the system can force them to a defined safe state (e.g., during a system failure), then those inputs need not meet this criterion)

- for systems with analog inputs, every combination of inputs over the entire operational range of the analog inputs, including defined over-range and

under-range conditions

- every possible executable logic path (includes nonsequential logic paths)
- every functional state transition among all modes of operation
- testing results that conform to preestablished test cases to monitor for correctness of all outputs for every case

b. Testing for latent design defects was conducted on a system that accurately represents the system to be installed, guaranteeing that the system installed will perform the same functions as the system tested.

c. Testing results account for potential spurious operations.

3.1.3 Use of Alternative Approaches Other Than Diversity and Testing to Eliminate the Potential for Common-Cause Failure from Further Consideration

Applicants may propose technical approaches to address CCF that this BTP does not describe. These may be design techniques, prevention measures, or mitigation measures other than diversity. The reviewer should determine whether an application requesting the use of an approach not described in this BTP includes a sufficient supporting technical basis, conditions of use, and acceptance criteria for its implementation.

The NRC staff can approve methods through guidance (e.g., endorsement of a standard) or a safety evaluation (e.g., precedent, topical report). Generally, the review of the implementation of a method previously approved by the NRC consists of (1) ensuring the method is implemented in a manner that is consistent with the purpose and conditions of use for which it was approved and (2) ensuring that adequate justification is provided for any deviations from the approved method.

If the application credits an approach not previously approved by the NRC, the reviewer should determine the acceptability of the proposed method in accordance with the acceptance criteria described below.

Generally, the proposal of an approach other than diversity should consist of (1) a description of its purpose and conditions of use, (2) a description of the method, (3) criteria for determining that the method will achieve its purpose, and (4) supporting information and reasoning demonstrating that the applicant's implementation satisfies these criteria with appropriate means to address the CCF.

<u>Acceptance Criteria for Use of a Proposed Alternative Approach</u>

If an application proposes an alternative approach to eliminate a CCF from further consideration, the reviewer should conclude that the application provides sufficient information on the alternative approach if the application includes all of the following:

a. the identification of the CCF vulnerabilities or causes that the proposed alternative approach addresses; if these are identified using a hazard analysis technique, then it should be confirmed independently that the analysis is correct and complete

b. a description (including supporting information and reasoning) of how the proposed alternative approach addresses the CCF vulnerabilities or causes and any potential spurious operations, including any conditions or limitations for the alternative approach

c. a technical basis explaining how the alternative approach addresses the identified CCF vulnerabilities or causes and prevents or mitigates their effects, including an analysis of how the methods' effectiveness will be demonstrated

3.1.4 Use of a Qualitative Assessment and Failure Analysis to Eliminate the Potential for Common-Cause Failure from Further Consideration

RIS 2002-22, Supplement 1, describes a methodology, called qualitative assessment, to assess the likelihood of failure due to CCF in DI&C systems and components. RIS 2002-22, Supplement 1, identifies acceptance criteria to determine whether a system has a low likelihood of failure such that current licensing assumptions continue to be met because the likelihood of CCF is much lower than other kinds of failures considered in the FSAR. This is referred to as "sufficiently low," and its definition compares the likelihood of failure of a proposed DI&C system or component to other failures documented in the FSAR.

The qualitative assessment is a less technically rigorous type of D3 assessment, and, as such, is sufficient to eliminate CCF vulnerabilities from further consideration only for systems of lower or lowest safety significance.

The qualitative assessment, as described in RIS 2002-22, Supplement 1, is a technical basis for demonstrating that a system will exhibit a low likelihood of failure (i.e., a low likelihood of CCF). The technical basis includes (1) three factors used to demonstrate that the proposed systems will exhibit a low likelihood of failure and (2) failure analyses (e.g., failure modes and effects analysis (FMEA), fault tree analysis (FTA)) to support the qualitative assessment. First, the reviewer should consider the factors used in the qualitative assessment to demonstrate that a DI&C system or component will exhibit a low likelihood of failure (i.e., low likelihood of CCF). The reviewer should confirm that the likelihood of failure of the proposed DI&C system or component remains consistent with assumptions in the licensing basis. A qualitative assessment should consider the following factors:

- the design attributes and features of the DI&C system or component
- the quality of the design process for the DI&C system or component
- any applicable operating experience for the DI&C system or component

Second, the reviewer should consider any failure analysis used in the qualitative assessment, including information from engineering design work, such as FMEAs and FTAs. The reviewer should consider whether the failure analysis supports the factors above and whether it demonstrates, for example, that identified potential CCFs exhibit a low likelihood of occurrence.

Acceptance Criteria for Use of Qualitative Assessment

If the acceptance criteria below are met, the reviewer should conclude that the application includes a qualitative assessment (consistent with the methodology described in RIS 2002-22, Supplement 1) that demonstrates that for SSCs of low safety significance, the likelihood of CCF is sufficiently low. The acceptance criteria are as follows:

a. The proposed system or component has design attributes and features that reduce the likelihood of CCFs.

b. The quality of the design process for the proposed system or component reduces the likelihood of CCFs, including CCFs potentially resulting in spurious operations.

c. The applicable operating experience collectively supports the conclusion that the proposed system or component will operate with high reliability for the intended application. In some cases, operating experience can compensate for uncertainties in addressing criteria (a) and (b).

d. The proposed system or component will not cause a failure or spurious operation that could invalidate the plant licensing basis (e.g., the maintenance of diverse systems for reactivity control).

e. The application documents the hazard analysis that demonstrates how hazardous effects, including spurious operations, are bounded or taken into account.

### 3.2 Use of Diverse Means to Mitigate the Impact of a Common-Cause Failure

This section addresses applications that credit a diverse means to accomplish the same or different function than the safety function disabled by the postulated CCF or to mitigate spurious operations resulting from the postulated CCF. Section 2.6 of NUREG/CR-6303 identifies 6 diversity attributes and 25 related diversity criteria that the reviewer can use to determine whether the diverse means are adequate to mitigate CCF. In addition, NUREG/CR-7007 identifies and develops a baseline set of diversity criteria that may characterize diversity strategies adequate to address CCF vulnerabilities. However, the quantification methodology described in NUREG/CR-7007 should not be used as the sole basis for justifying adequate diversity.

An application that credits any of the diverse means described in sections B.3.2.1–B.3.2.3 of this BTP is considered to have acceptably addressed Point 3 of the NRC position on D3. These diverse means include existing systems, manual operator actions, or new diverse systems.

#### 3.2.1 Crediting Existing Systems

An existing reliable I&C system can be used as a diverse means to accomplish the same or a different function credited in the D3 assessment or to mitigate spurious operations resulting from CCF. The analysis in the LAR of the function performed by this existing system should show that the consequences of the CCF meet the acceptance criteria defined in the FSAR or the LAR for the limiting events applicable to the proposed system or component. If an existing system is credited, then the reviewer should verify that the applicant performed an analysis demonstrating that the credited system and the proposed system are not both vulnerable to the same CCF.

The reviewer should verify that the applicant considered how the existing system is credited in the facility's licensing basis and described in the existing system's documentation (e.g., FSAR, detailed design documents). Among other things, the reviewer should consider whether the applicant has appropriately accounted for any unique system design attributes and requirements and potential interconnectivities, including resource sharing, to other systems. The reviewer should pay particular attention to whether there may be interconnectivities, including

resource sharing, the LAR has not accounted for that may result in the existing system being subject to the same CCF as the proposed DI&C system or component. The reviewer should verify that the application has identified all the features of the existing system that are relevant to demonstrating diversity. In addition, if crediting an existing system could affect the facility's existing licensing basis, then the reviewer should verify that the LAR addresses how the existing system functions would be credited and justified in a revised licensing basis.

The credited existing system may be a system that is not safety related, as long as it is of sufficient quality and can reliably perform the credited functions under the associated event conditions. If the applicant credits systems that are not safety related that are in continuous use (e.g., the normal reactor coolant system inventory control system or the normal steam generator level control system), these systems need not meet augmented quality standards. However, if the applicant credits systems that are not safety related and that are not in continuous use (i.e., that are normally in standby mode), then the reviewer should verify that the applicant demonstrated that the system will reliably perform its intended function. For example, the applicant may credit the plant ATWS system as a diverse means of achieving reactor shutdown, provided that the ATWS system is capable of responding to the same analyzed events as the proposed DI&C system. In this case, the reviewer should consider whether the D3 analysis demonstrates that the ATWS system (1) is not vulnerable to the same CCF as the equipment performing the reactor trip function within the proposed DI&C system, (2) is of sufficient quality and is capable of functioning under the event conditions expected, and (3) is responsive to the AOO or PA sequences.

If prioritization is used, the reviewer should verify that signals to actuate components coming from the new use of the credited existing system and other systems are adequately prioritized to ensure the overall defense-in-depth strategy and existing licensing basis is maintained. The reviewer should also verify that changes to an existing prioritization scheme due to the new use of the credited system are consistent with the existing licensing basis. If there are shared resources (e.g., priority modules), the reviewer should consider whether the credited existing system has priority over the resources in regard to its safety and protection functions, such that these functions are always carried out first. RG 1.152 provides guidance on prioritization of control and protection systems sharing components. (In some cases, certain components may have more than one safe state; the reviewer should consider whether all safe states were described in the priority scheme.)

Acceptance Criteria for Crediting Existing Systems

If the acceptance criteria below are met, the reviewer should conclude that the application includes a D3 assessment justifying the use of an existing plant system as a diverse means. The existing system may perform the same function as that disabled by the postulated CCF, or it may perform a different function to compensate for or mitigate the loss of the disabled function. The acceptance criteria are as follows:

a. If the diverse system uses equipment that is not safety related, the equipment is of sufficient quality to perform the necessary function(s) during the associated event conditions. Sufficient quality can be achieved, for example, through application of the alternative treatment requirements developed for implementation of 10 CFR 50.69 or the ATWS quality assurance guidance in GL 85-06.

b. Sufficient diversity exists between the diverse system and the proposed system, so that

they are not subject to the same postulated CCF.

c. The equipment to be credited has functional capabilities sufficient to maintain the plant within the acceptance criteria defined in the FSAR or the LAR for the limiting events applicable to the proposed DI&C system or component.

d. The LAR maintains the existing system's licensing basis in view of the new credited use, or the LAR identifies and analyzes those parts of the existing system's licensing basis being updated as a result of the proposed change.

e. If prioritization is used, the new use of the credited system maintains the existing prioritization scheme. If the new use of the existing system results in changes to the existing prioritization scheme, the changes are consistent with the plant's licensing basis, and safety and protection functions have the highest priority when resources are shared. The commands to actuate components resulting from safety and protection are always performed over other functions.

3.2.2 Crediting Manual Operator Action

When addressing Point 3, the applicant may credit a manual operator action as a diverse means to accomplish the same or a different function credited in the D3 assessment or to mitigate spurious operation. To be creditable, manual operator actions should be performed within a time frame adequate to effectively mitigate the event. In addition, a human factors evaluation process, such as the process outlined in SRP Chapter 18, should show that the proposed manual operator action is both feasible and reliable. The reviewer may use a risk-informed approach to determine the appropriate level of HFE review needed for proposed changes to existing credited manual actions or for proposed new manual operator actions.

The reviewer should consider whether the equipment necessary to perform these actions, including the supporting indications and controls, is diverse from (i.e., not vulnerable to the same sources of CCF as) the equipment performing the same function within the safety-related I&C system. If the equipment used to perform the credited manual operator action is not safety related, then the applicant should demonstrate that the equipment is of adequate quality—for example, by applying the alternative treatment requirements in 10 CFR 50.69 or the ATWS quality assurance guidance in GL 85-06.

If the applicant proposed the use of equipment outside the MCR to perform the credited manual operator action, the reviewer should consider whether this equipment is vulnerable to the same CCF as the safety system and whether the applicant demonstrated that the equipment will be reliable, available, and accessible under the postulated event conditions. The reviewer may use the HFE principles and criteria identified in SRP Chapter 18 to evaluate the applicant's selection and design of the displays and controls. In addition, the reviewer may use the guidance in NUREG-1764, Revision 1, "Guidance for the Review of Changes to Human Actions," issued September 2007, to perform a risk-informed evaluation of the application.

<u>Protective Actions Initiated Solely by Manual Actions</u>

For protective actions initiated solely by manual controls consider appropriate HFE criteria and adequate equipment and controls. RG 1.62 provides guidance for evaluating the adequacy of

equipment and controls used to manually initiate protective actions otherwise provided by automatically initiated safety systems. SRP Chapter 18 provides guidance for evaluating credited manual actions.

Acceptance Criteria for Manual Actions

If the following acceptance criteria are met, the reviewer should conclude that the proposed manual operator action is acceptable:

a. The proposed manual operator action has been validated as both feasible and reliable, using an HFE process such as that specified in SRP Chapter 18. The application describes human performance requirements and relates them to the plant safety criteria. The application employs recognized human factors standards and design techniques to support the described human performance requirements.

b. The SSCs used to support the manual operator action are diverse from the equipment performing the same function within the DI&C system, so that they are not vulnerable to the same CCFs.

c. The credited SSC is accessible to the operator during the associated event conditions, is capable of functioning under the expected conditions, and is of adequate quality, which may be verified, for example, based on the alternative treatment requirements developed for implementation of 10 CFR 50.69, or on the ATWS quality assurance guidance in GL 85-06.

d. The indications and controls needed to support the manual operator action have the functional characteristics necessary to maintain the plant within the facility operating limits.

3.2.3 Crediting a New Diverse System

The applicant may propose a new diverse system (e.g., a diverse actuation system) as a diverse means of accomplishing the same or a different function credited in the D3 assessment or of mitigating spurious operation due to CCF. In this case, the reviewer should determine whether the application demonstrates that (1) the functions performed by this diverse means suffice to maintain plant conditions within specified acceptance criteria for the associated DBE, and (2) sufficient diversity exists between the new system and the proposed DI&C system so that they are not vulnerable to the same postulated CCF. The reviewer should determine whether the diverse means credited and the digital design of the proposed system are vulnerable to the same CCF.

The new diverse system may be a system that is not safety related if it is of sufficient quality to perform the necessary functions under the associated event conditions. The reviewer should consider whether the new diverse system can function under the event conditions expected and whether it is of adequate quality, which can be verified, for example, based on the alternative treatment requirements developed for implementation of 10 CFR 50.69, or on the ATWS quality assurance guidance in GL 85-06.

Prioritization

If a new diverse system is implemented, the reviewer should verify that the signals to actuate

components coming from the different systems are appropriately prioritized to maintain the overall defense-in-depth strategy. If the proposed DI&C system and the new diverse system share resources (e.g., priority modules), the reviewer should consider whether the proposed DI&C system has priority in the use of shared resources in regard to its safety and protection functions, so that safety and protection functions are always carried out first. RG 1.152 provides guidance on prioritization of control and protection systems sharing components. (In some cases, certain components may have more than one safe state; the reviewer should consider whether the priority scheme describes all safe states.)

Acceptance Criteria for Crediting a New Diverse System

If the following acceptance criteria are met, the reviewer should conclude that the use of a new diverse system is acceptable:

a. If the diverse system uses equipment that is not safety related, the equipment is of sufficient quality to perform the necessary function(s) during the associated event conditions. Sufficient quality can be achieved, for example, through application of the alternative treatment requirements developed for implementation of 10 CFR 50.69 or the ATWS quality assurance guidance in GL 85-06.

b. Sufficient diversity exists between the diverse system and the proposed system, so that they are not vulnerable to the same postulated CCF.

c. The equipment credited has functional capabilities sufficient to maintain the plant within the acceptance criteria defined in the FSAR or the LAR for the limiting events applicable to the proposed system or component.

d. Resources shared by proposed system(s), other systems, and manual operator actions are controlled by prioritization of commands consistent with the guidance in RG 1.152. The basis for the prioritization should be documented.

3.3 Consequences of a Common-Cause Failure May Be Acceptable

This section addresses applications that propose consequences of a residual identified CCF remain acceptable. In this case, the reviewer should consider whether the applicant's analysis demonstrates that, should the CCF occur, the facility will remain within the acceptance criteria defined in the FSAR or the LAR for the limiting events applicable to the proposed DI&C system or component.

For each event analyzed in the accident analysis, the applicant may perform the D3 assessment using either best estimate methods (i.e., using realistic assumptions to analyze the plant's response to DBEs) or conservative methods (i.e., design-basis analysis). The reviewer should consider whether the D3 assessment shows that the consequences of potential CCFs of the proposed system, or of portions of the proposed system, are acceptable.

Acceptance Criteria for Determination of Acceptable Consequences

If the acceptance criteria below are met, the reviewer should conclude that the application shows that the consequences of potential CCFs of the proposed system or portions of the proposed system are acceptable. The acceptance criteria are as follows:

a. For those postulated spurious operations that have not been fully mitigated or eliminated from further consideration, the consequences of spurious operation of safety-related components or components that are not safety related are bounded by the acceptance criteria defined in the FSAR or the LAR.

b. For each AOO in the design basis that occurs concurrently with the CCF, the plant response, calculated using realistic or conservative assumptions, does not result in radiation release exceeding 10 percent of the applicable dose guideline values, or a loss of integrity of the primary coolant pressure boundary.

c. For each PA in the design basis that occurs concurrently with each single postulated CCF, the plant response, calculated using realistic or conservative assumptions, does not result in radiation release exceeding the applicable dose guideline values, in violation of the integrity of the primary coolant pressure boundary, or in violation of the integrity of the containment.

### 3.4 Risk-Informed Diversity and Defense-in-Depth Assessment

A risk-informed approach to address a CCF generally consists of (1) analyzing the functional impact of the CCF, (2) determining the risk significance of the CCF, and (3) determining appropriate means to address the CCF commensurate with the risk significance of the CCF.

Point 1 of the policy refers to the risk significance of the DI&C system. Under Point 1, the D3 assessment must be commensurate with the risk significance of the system. It is possible for a system to be risk significant due to the combined effects of system functions, hidden interdependencies, corresponding interactions, and emergent behaviors, even if each system function alone may not be risk significant. Therefore, when there is potential for such behaviors, correspondingly more comprehensive modeling and evaluation of the plant are needed.

Point 3 of the policy, however, refers to the risk significance of a CCF. Under Point 3, one option is for the D3 assessment to demonstrate that a postulated CCF is not risk significant. While the risk significance of the DI&C system is different from the risk significance of a CCF, the same causes may degrade different safety functions, thus increasing the risk significance of the CCF beyond the increase in risk from the loss of a single safety function. Therefore, when there is potential for such behaviors, correspondingly more comprehensive evaluation of the plant is needed.

Risk significance and safety significance are different concepts. NUREG-2122, “Glossary of Risk-Related Terms in Support of Risk-Informed Decisionmaking,” issued November 2013, states the following:

> A principal focus of a PRA is to determine the risk significance of the various “features,” i.e., the systems, structures, and components (SSCs), human actions or the accident sequences involving those SSCs, of the facility being analyzed. Usually, an item is considered risk significant when the risk associated with it exceeds a predetermined limit for contributing to the risk associated with the facility. Since the overall risk of a nuclear facility can be calculated in terms of core damage frequency (CDF) (Level 1 PRA), or releases (Level 2 PRA), or health effects (Level 3 PRA), risk significance can also be determined as related to these various risk measures.

NUREG-2122 also states that the term “risk significant” does not have the same meaning as the term “safety significant,” and safety significance is not evaluated in a PRA.

This distinction between risk significance and safety significance is used, in part, to emphasize the need to consider safety margins when applications use a risk-informed approach since the application should not overly rely on the changes in CDF and large early release frequency (LERF) alone.

Section B.3.4.4 describes how the risk significance of a CCF, as opposed to the safety significance of the SSC, is used in part to determine appropriate means to address the CCF. Because a risk-informed approach considers other factors to determine acceptability, the reviewer should ensure that applications using a risk-informed approach demonstrate sufficient safety margins exist so that DI&C and associated D3 systems remain capable of performing their safety functions.

Section C.2.1.2 of RG 1.174 provides guidance on ensuring that designs possess sufficient safety margins. With sufficient safety margins, (1) the codes and standards or their alternatives approved for use by the NRC are met and (2) safety analysis acceptance criteria in the licensing basis (e.g., FSAR, supporting analyses) are met or proposed revisions provide sufficient margin to account for uncertainty in the analysis and data.

### 3.4.1 Determining Consistency with NRC Policy and Guidance on Risk-Informed Decision-Making

Point 2 of the policy states that applicants using a risk-informed approach must include an evaluation of the approach against the Commission’s policy and guidance, including any applicable regulations, for risk-informed decision-making. Point 2 also states that the NRC staff will review applications that use risk-informed approaches for consistency with established NRC policy and guidance on risk-informed decision-making, and it provides RG 1.174 as an example.

RG 1.174 describes an approach that is acceptable to the NRC staff for developing risk-informed applications for a licensing basis change. RG 1.174 references RG 1.200, which provides an approach for determining whether the base PRA (in total or the parts that are used to support an application) is acceptable for use in regulatory decision-making.

If an application uses a risk-informed approach to address a CCF, the reviewer should follow current NRC staff review guidance (including SRP Chapter 19, “Severe Accidents,” or final interim staff guidance (ISG) DC/COL-ISG-028, “Assessing the Technical Adequacy of the Advanced Light-Water Reactor Probabilistic Risk Assessment for the Design Certification Application and Combined License Application,” issued November 2016) to confirm that the risk-informed approach is consistent with the Commission’s policy and guidance.

Acceptance Criteria for Determining Consistency with NRC Policy and Guidance on Risk-Informed Decision-Making

If the application meets the acceptance criteria in the applicable NRC staff review guidance for risk-informed applications and addresses the five principles of risk-informed decision-making in RG 1.174, the reviewer should conclude that the application provides sufficient information to conclude that the risk-informed approach is consistent with the established NRC policy and guidance on risk-informed decision-making.

### 3.4.2 Modeling the Common-Cause Failure

It is important for reviewers to understand the limitations associated with some PRA models related to CCFs. One limitation is that some PRA models do not include details of various hardware or software components of DI&C systems or all the interdependencies across different SSCs.

If an application uses a plant-specific PRA as part of its risk-informed approach to address a CCF, the reviewer should determine whether the application is based on a base PRA that meets the PRA acceptability guidance in RG 1.200 or equivalent guidance for new reactors such as DC/COL-ISG-028. The application should justify the exclusion of any PRA hazard or operating mode from the risk-informed D3 assessment. The application should also justify any changes beyond those for modeling the CCF made to the PRA model to support the application, including whether the changes are considered PRA maintenance or a PRA upgrade (typically based on the corresponding definitions in the application's specified revision of RG 1.200 or equivalent guidance for new reactors, such as DC/COL-ISG-028).

A change made to a PRA model may involve PRA maintenance or a PRA upgrade, which includes the use of a newly developed method. RG 1.200 provides guidance for classifying changes to a PRA model as PRA maintenance or a PRA upgrade. The reviewer should consider any guidance used (e.g., the specific revision of RG 1.200 or DC/COL-ISG-028) for configuration control of the PRA supporting the application and confirm whether any changes made to the PRA model are PRA maintenance or a PRA upgrade based on the corresponding definition in the identified guidance. SRP Section 19.2, "Review of Risk Information Used to Support Permanent Plant-Specific Changes to the Licensing Basis: General Guidance," provides review guidance for performing a focused-scope review of the risk analysis on an application-specific basis, as needed.

The reviewer should determine whether the application explains how the CCF is modeled in the PRA and provides justification that the modeling includes the impact of the CCF. In providing the justification, the application should evaluate DI&C system interconnectivity and address DI&C system spatial separation that could significantly influence the risk due to fires, earthquakes, and other hazards. This can be accomplished through detailed modeling of the DI&C system in the PRA or the use of surrogate events, which can be existing basic events in the PRA or new basic events added to the PRA that include the impact of the CCF on the plant. The application may address each CCF using a different approach (i.e., the application may address some CCFs through detailed modeling of the DI&C system and other CCFs using surrogate events).

SRP Section 19.0, "Probabilistic Risk Assessment and Severe Accident Evaluation for New Reactors," provides guidance for reviewing DI&C system risk assessments for new reactors, which may also be applicable to operating reactors.

Since a CCF could affect a single plant system or function or multiple plant systems or functions, considerable care should be taken when reviewing how the CCF is modeled. The I&C technical reviewer and risk analyst should coordinate the review to ensure that the application sufficiently addresses the impact of the CCF on plant systems and functions.

Acceptance Criteria for Modeling the Common-Cause Failure

If the application meets the following acceptance criteria, the reviewer should conclude that the application provides sufficient information on modeling the CCF to determine its risk significance. The acceptance criteria are as follows:

a. The application identifies the basis for the technical acceptability of the base PRA (e.g., a specific revision of RG 1.200 or equivalent guidance for new reactors, such as DC/COL-ISG-028) used for the risk-informed D3 assessment, demonstrates that the base PRA is technically acceptable, and reflects the plant or design at the time of the application.

b. The exclusion of any PRA hazard or operating modes from the risk-informed D3 assessment is adequately justified.

c. Adequate justification is provided for any changes to the PRA model to support the application (e.g., whether the changes are considered PRA maintenance or a PRA upgrade based on the corresponding definitions in the revision of RG 1.200 or equivalent guidance for new reactors, such as DC/COL-ISG-028, identified in the application).

d. For an application addressing a CCF through detailed modeling of the DI&C system in the PRA—

    i. the CCF is modeled in sufficient detail, including intersystem and intrasystem dependencies and associated potential emergent behaviors, to evaluate the impact of the CCF on plant equipment and functions modeled in the PRA (including the ability for operators to perform manual actions), and

    ii. adequate justification is provided that the impact of the CCF on plant equipment and functions not modeled in the PRA is not risk significant.

e. For an application addressing a CCF using surrogate events—

    i. the surrogate events bound the impact of the CCF on plant equipment, functions, and operator actions modeled in the PRA, and

    ii. adequate justification is provided that the impact of the CCF on plant equipment, functions, and operator actions not modeled in the PRA is not risk significant.

f. Key assumptions and sources of uncertainty impacting the application are identified and dispositioned following established guidance such as RG 1.200 or equivalent guidance for new reactors and NUREG-1855, Revision 1, “Guidance on the Treatment of Uncertainties Associated with PRAs in Risk-Informed Decisionmaking,” issued March 2017.

3.4.3 Determining the Risk Significance of the Common-Cause Failure

The risk significance of a CCF can be determined using a bounding sensitivity analysis that assumes the probability of the CCF is 1 or a sensitivity analysis that uses a conservative value less than 1 for the probability of the CCF.

In some situations, a CCF may not disable a protective function (e.g., a CCF associated with the upgrade from analog to digital control room annunciators), but it may affect operators' ability to perform required actions. In these situations, the risk significance of the CCF can be determined by modeling the operators' failure to perform required actions and conducting a bounding sensitivity analysis (assuming a probability of 1) or recalculating the applicable human error probabilities with supporting technical justification for the recalculated values (e.g., if there are other indicators present that will allow operators to detect and diagnose the plant status).

Acceptance Criteria for Determining the Risk Significance of the Common-Cause Failure

If the application meets the acceptance criteria, which are used in conjunction with information in the application on the principles of risk-informed decision-making in RG 1.174, the reviewer should conclude that the application provides sufficient information on determining the risk significance of the CCF. The acceptance criteria are as follows:

a. If the increase in risk from the CCF is calculated using a bounding sensitivity analysis, the bounding sensitivity analysis presumes that the CCF occurs (i.e., the probability of failure of the surrogate events is 1) and describes the baseline risk used to determine the increase in risk (e.g., basis for the nominal failure probability for the CCF used in the baseline model is zero (i.e., the CCF does not occur in the baseline model)).

b. If the increase in risk from the CCF is calculated using a sensitivity analysis that includes a conservative value for the probability of a CCF, the application—

    i. provides a technical basis that demonstrates that an adequate level of defense in depth is provided for the conservative probability less than 1, and

    ii. assesses the impact of this assumption on PRA uncertainty, including a determination of whether it is a key assumption, and the key principles of risk-informed decision-making, including defense in depth.

c. The risk quantification accounts for any dependencies introduced by the CCF, including the ability for operators to perform manual actions.

The following acceptance criteria, which are to be used in conjunction with information in the application on the principles of risk-informed decision-making in RG 1.174, apply for CCFs determined to be not risk significant:

a. The increase in CDF from the CCF is less than $1 \times 10^{-6}$/year.

b. The increase in LERF from the CCF is less than $1 \times 10^{-7}$/year.

3.4.4 Determining Appropriate Means to Address the Common-Cause Failure

Point 3 of the policy states that applicants must demonstrate the adequacy of any design techniques, prevention measures, or mitigation measures, other than diversity, that are credited in the assessment. Point 3 also states that the level of technical justification demonstrating the adequacy of these techniques or measures, other than diversity, to address CCFs must be commensurate with the risk significance of each CCF.

For the CCFs that are determined to be risk significant, the level of technical justification needed can be determined by mapping the increase in risk from the CCF to the acceptance guidelines in RG 1.174. For example, a higher level of technical justification is needed for CCFs that fall in Region I versus those that fall in Region II of figures 4 or 5 in RG 1.174. The most recent plant-specific CDF and LERF should be used for the mapping.

Acceptance Criteria for Determining the Appropriate Means to Address the Common-Cause Failure

If a CCF is not risk significant (i.e., the increase in risk from the CCF falls in Region III of figures 4 and 5 of RG 1.174), then the reviewer should conclude that standard design and verification and validation processes are sufficient to address the CCF. If a CCF is risk significant and the application meets the acceptance criteria below, with a level of technical justification commensurate with the risk significance of the CCF (as characterized by mapping its increase in risk to the regions in RG 1.174), the reviewer should conclude that appropriate means to address the CCF have been applied:

a. The application identifies the CCF vulnerabilities or causes; if these are identified using a hazard analysis technique, then it should be confirmed independently that the analysis is correct and complete.

b. A description (including supporting information and reasoning) of how the application addresses the CCF vulnerabilities or causes and any potential spurious operations, including any conditions or limitations.

c. A technical basis explaining how the application addresses the identified CCF vulnerabilities or causes and prevents or mitigates their effects, including an analysis of how the effectiveness of the methods used in the application will be demonstrated.

4. Manual System-Level Actuation and Indications to Address Point 4

Point 4 of the policy states that MCR displays and controls that are independent and diverse from the proposed DI&C system (i.e., unlikely to be subject to the same CCF) must be provided for manual system-level actuation of critical safety functions (which may have been determined using risk information) and monitoring of parameters that support the safety functions. Section B.1.2 provides information on critical safety functions. RG 1.62 outlines important design criteria for I&C equipment used by plant operators for manual initiation of protective actions. Point 4 also states that the applicant may alternatively propose a different approach to this point in the policy if the plant design has a commensurate level of safety.

The reviewer should consider whether displays and manual controls provided to meet Point 4 are not vulnerable to the same CCF as the proposed DI&C system. For example, the point at which the credited manual controls are connected to the safety equipment should be downstream of the equipment that can be adversely affected by a CCF.

Point 4 specifies that the independent and diverse MCR displays and controls may be used to address Point 3.If the displays and manual controls provided to meet Point 4 are not vulnerable to the same CCF as the proposed DI&C system, the applicant may credit them as the diverse means called for under Point 3. In most cases, when displays and manual controls are credited

as the diverse means for Point 3, they may also be credited for Point 4. However, if the diverse means credited for Point 3 are not located in the MCR, then they are not sufficient to meet Point 4.

The reviewer should determine whether controls outside the MCR are exclusively used for long-term management of the critical safety functions after completion of system-level or division-level manual actuation from the MCR using the Point 4 displays and controls. The reviewer should also determine whether controls outside the MCR are supported by suitable HFE analysis and site-specific procedures or instructions.

Acceptance Criteria

If the following acceptance criteria are met, the reviewer should conclude that the manual controls and supporting displays meet Point 4:

a. The proposed manual actions credited to accomplish safety functions that would otherwise have been accomplished by automatic safety systems are both feasible and reliable, as demonstrated through an HFE analysis and assessment process, such as the one described in SRP Chapter 18.

b. The application identifies the minimum inventory of displays and controls in the MCR, and this minimum inventory allows the operator to effectively actuate, monitor, and control the critical safety function parameters (e.g., reactivity, core heat removal, reactor coolant inventory, containment isolation, and containment integrity).

c. The proposed manual operator actions are prescribed by licensee-approved plant procedures and subject to appropriate training.

d. The manual controls for critical safety functions are at the system or division level and are located within the MCR. 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.

e. If equipment that is not safety related is used, its quality and reliability are adequate to support the manual operator action during the associated event conditions. Equipment quality can be verified, for example, based on the alternative treatment requirements developed for implementation of 10 CFR 50.69, or on the ATWS quality assurance guidance in GL 85-06.

f. The displays and controls are independent and diverse from the equipment performing the same functions within the proposed safety-related DI&C systems. These displays and controls are not affected by postulated CCFs that could disable the corresponding functions within the proposed safety-related DI&C systems.

For applications that propose a different approach for meeting Point 4, acceptance criteria items a, c, e, and f, above are generally applicable regardless of the location of equipment that perform specific critical safety functions, and would likely be relevant to most applications. The reviewer should determine whether applications for different approaches that do not meet all the acceptance criteria items above contain appropriate justification that the plant design has a commensurate level of safety comparable to the level of safety provided by ensuring operators'

ability to monitor, initiate, and control the applicable critical safety function parameters is maintained.

5. Information for Interdisciplinary NRC Staff Review

In addition to conducting the review described in the preceding sections, the reviewer should also work with NRC staff in other disciplines to identify other areas that may be affected by CCFs. The technical staff should review the following for potential interdisciplinary concerns:

- the applicant's documentation of its safety-significance determination for a proposed DI&C system and the supporting technical basis, with risk analysts reviewing the details of a risk-informed approach or risk insights supported by a plant-specific PRA if used in the D3 assessment

- the results of any D3 assessment, including consideration of spurious operations, and specifically the following:

  – any means used to eliminate potential CCFs from further consideration, any information demonstrating that these means are effective, and any remaining CCF vulnerabilities (residual risks)

  – any diverse means provided by the applicant to accomplish the same or a different function than the safety function disabled by a postulated CCF for any CCFs not eliminated from further consideration using design attributes (if any diverse means is credited to mitigate the potential CCF, the information provided to demonstrate the effectiveness of the diverse means, including assessment from the results of HFE analysis associated with any manual operator actions used as a diverse means)

  – verification of the acceptability of the results of any consequence analysis that the applicant has performed for CCFs not eliminated from further consideration or mitigated using diverse means, with such an analysis demonstrating that the consequences of the CCF are within acceptable limits for each AOO and PA

- for systems that the applicant has not assessed for CCF, information showing that all conditions introduced by the proposed modification are bounded by the acceptance criteria defined in the FSAR or the LAR for the limiting events applicable to the proposed DI&C system or component

- for manual system-level actuation and indications to address Point 4, design information showing the following:

  – controls and displays are provided in the MCR to perform manual system- or division-level actuation of critical safety functions

  – the controls and displays are independent and diverse from the equipment performing the same functions within the proposed DI&C system, so that they are not vulnerable to the same CCF as the proposed system

  – the controls and displays have sufficient quality to support the manual operator

actions during the associated event conditions, if the equipment used is not safety related

## 6. Additional Items for Consideration

The reviewer should use the acceptance criteria described in this BTP to evaluate the applicant's D3 assessment. During this evaluation, the reviewer should consider the topics described below.

### 6.1 System Representation as Blocks

A block is a representation of a physical subset of equipment and software for which it can be credibly assumed that internal failures, including the effects of latent design defects, will not propagate to equipment or software outside of the block. A block can also be a software macro or subroutine, such as a voting block or a proportional–integral–derivative block, that is used by multiple functional applications. Representations of systems or components using blocks may not show the inner workings of each block.

Typical examples of blocks are computers, local area networks, software macros and subroutines, and programmable logic controllers. When a block is used by multiple design functions using the same software (within the logic or divisions), a failure within the block can result in a CCF of all design functions that use that block.

The reviewer should consider whether the applicant's D3 assessment describes the diversity of the proposed DI&C system or component across blocks. When considering the effects of a postulated CCF, the reviewer may assume that the diverse blocks function as designed. This includes blocks that act to prevent or mitigate consequences of the CCF under consideration.

### 6.2 Documentation of Assumptions

The reviewer should verify that the application documents and justifies any assumptions made to compensate for missing information in the design description materials or to explain interpretations of the analysis guidelines applied to the system.

### 6.3 Identification of Alternate Trip or Initiation Sequences

The reviewer should verify that the applicant's assessment includes analyses of the sequence of events that would occur if the primary trip channel failed to trip the reactor or actuate engineered safety features. The analyses may use realistic or conservative (design-basis) assumptions. When evaluating these analyses, the reviewer should coordinate with the NRC staff organization responsible for the review of reactor systems, or PRA-based applications.

### 6.4 Identification of Alternative Mitigation Capability

For each CCF, the reviewer should verify that the applicant has identified alternative mitigation actuation functions or design techniques that will prevent or mitigate core damage and unacceptable release of radioactivity. If a potential CCF in an automatic or manual function credited in the plant accident analysis is compensated for by a different automatic or manual function, the applicant should provide a basis demonstrating that the different function constitutes adequate mitigation in the event conditions.

If the application cites a manual operator action as a diverse means for responding to an event, the reviewer should verify that the applicant's HFE analysis and assessment demonstrate (e.g., through the process in SRP Chapter 18) that this action is both feasible and reliable. For this, the reviewer should coordinate with the organization responsible for the review of human-system interfaces.

6.5 Justification for Not Correcting Specific Vulnerabilities

The reviewer should consider whether the applicant provided justification for not correcting any identified vulnerabilities that the application leaves unresolved. Such justification might include, for example, design attributes (e.g., redundancy, diversity, independence) and diverse actuation or mitigation capabilities, as well as previously NRC-approved credited manual operator actions in the licensing basis to address AOOs or PAs. The NRC staff should review justifications on a case-by-case basis. For example, an applicant might credit the ability of plant operators to identify system leakage using the plant leak detection system before the onset of a large-break pipe rupture. The crediting of such manual operator actions could be justified by appropriate analysis of site-specific factors such as pipe configuration and design, piping fracture mechanics, leak detection system capabilities, and details of manual operator actions and procedures. The reviewer should consider whether evaluation of the applicant's justifications necessitates a multidisciplinary review in cooperation with other NRC staff.

## C. REFERENCES


1. NRC, NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition" (SRP), Section 7.1-T, "Table 7-1 Regulatory Requirements, Acceptance Criteria, and Guidelines for Instrumentation and Control Systems Important to Safety"

2. NRC, RG 1.70, "Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants: LWR Edition"

3. 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities"

4. 10 CFR Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants"

5. 10 CFR Part 100, "Reactor Site Criteria"

6. IEEE Std 279-1968, "Proposed IEEE Criteria for Nuclear Power Plant Protection Systems," Piscataway, NJ, August 1968

7. IEEE Std 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations," Piscataway, NJ, June 1971

8. IEEE Std 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," Piscataway, NJ, June 1991

9. IEEE Std 603-1991, "Standard Criteria for Safety Systems for Nuclear Power Generating Stations," Correction Sheet, Piscataway, NJ, January 30, 1995

10. NRC, RG 1.233, “Guidance for a Technology-Inclusive, Risk-Informed, and Performance-Based Methodology to Inform the Licensing Basis and Content of Applications for Licenses, Certifications, and Approvals for Non-Light-Water Reactors”

11. NRC, RG 1.62, “Manual Initiation of Protective Actions”

12. NRC, RG 1.53, “Application of the Single-Failure Criterion to Safety Systems”

13. NRC, RG 1.152, “Criteria for Programmable Digital Device in Safety-Related Systems of Nuclear Power Plants”

14. NRC, RG 1.174, “An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis”

15. NRC, NUREG-0800, SRP Chapter 19, “Severe Accidents”

16. NRC, NUREG-0800, SRP Section 19.0, Revision 3, “Probabilistic Risk Assessment and Severe Accident Evaluation for New Reactors,” December 2015 (ML15089A068)

17. NRC, NUREG-0800, SRP Section 19.2, “Review of Risk Information Used to Support Permanent Plant-Specific Changes to the Licensing Basis: General Guidance”

18. NRC, DC/COL-ISG-028, “Assessing the Technical Adequacy of the Advanced Light-Water Reactor Probabilistic Risk Assessment for the Design Certification Application and Combined License Application,” November 2016 (ML16130A468)

19. NRC, RG 5.71, “Cybersecurity Programs for Nuclear Power Reactors”

20. NRC, NUREG-0800, SRP Section 7.7, “Control Systems”

21. NRC, NUREG-0800, SRP Section 7.8, “Diverse Instrumentation and Control Systems”

22. NRC, NUREG-0800, SRP Section 13.6.6, “Cyber Security Plan”

23. NRC, NUREG-0800, SRP Chapter 18, “Human Factors Engineering”

24. NRC, NUREG-0800, Appendix 7.0-A, “Review Process for Digital Instrumentation and Control Systems”

25. NRC, NUREG-0800, SRP BTP 7-17, “Guidance on Self-Test and Surveillance Test Provisions”

26. NRC, NUREG-0800, SRP BTP 7-21, “Guidance on Digital Computer Real-Time Performance”

27. NRC, NUREG-1764, Revision 1, “Guidance for the Review of Changes to Human Actions,” September 2007 (ML072640413)

28. NRC, NUREG/CR-7007, “Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems,” February 2010 (ML100880143)

29. NRC, NUREG/CR-6303, “Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems,” December 1994 (ML071790509)

30. NRC, SECY-93-087, “Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs,” April 2, 1993 (ML003708021)

31. NRC, SRM-SECY-93-087, “SECY-93-087—Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs,” July 21, 1993 (ML18145A018)

32. NRC, SECY-18-0090, “Plan for Addressing Potential Common Cause Failure in Digital Instrumentation and Controls,” September 12, 2018 (ML18179A066)

33. NRC, Generic Letter 85-06, “Quality Assurance Guidance for ATWS Equipment that Is Not Safety-Related,” April 16, 1985 (ML031140390)

34. NRC, 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 (ML18143B633)

35. RG 1.200, “Acceptability of Probabilistic Risk Assessment Results for Risk-Informed Activities”

36. NRC, NUREG-1855, Revision 1, “Guidance on the Treatment of Uncertainties Associated with PRAs in Risk-Informed Decisionmaking,” March 2017 (ML17062A466)

37. NRC, SECY-22-0076, “Expansion of Current Policy on Potential Common-Cause Failures in Digital Instrumentation and Control Systems,” August 10, 2022 (ML22193A290)

38. NRC, “Supplement to SECY-22-0076, ‘Expansion of Current Policy on Potential Common Cause Failures in Digital Instrumentation and Control Systems,’” January 23, 2023 (ML22357A037)

39. NRC, SRM-SECY-22-0076, “Staff Requirements—SECY-22-0076—Expansion of Current Policy on Potential Common-Cause Failures in Digital Instrumentation and Control Systems,” May 25, 2023 (ML23145A181 and ML23145A182)

40. NRC, BTP 7-19, Revision 8, “Guidance for Evaluation of Defense in Depth and Diversity to Address Common-Cause Failure Due to Latent Design Defects in Digital Safety Systems,” January 2021 (ML20339A647)

41. NRC, RG 1.97, Revision 4, “Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants,” June 2006 (ML061580448)

42. NRC, RG 1.97, Revision 5, “Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants,” April 2019 (ML18136A762)

43. NRC, NUREG-2122, “Glossary of Risk-Related Terms in Support of Risk-Informed Decisionmaking,” November 2013 (ML13311A353)

**Paperwork Reduction Act**

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 collections were approved by the Office of Management and Budget (OMB), under control numbers 3150-0011 and 3150-0151, respectively. Send comments regarding this information collection to the FOIA, Library, and Information Collections Branch (T6 A10M), U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001, or by email to Infocollects.Resource@nrc.gov, and to the Desk Officer, Office of Information and Regulatory Affairs, NEOB-10202 (3150-0011 and 3150-0151), Office of Management and Budget, Washington, DC 20503; email: 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, Draft Revision 9,**
**"Guidance For Evaluation of Defense in Depth and Diversity**
**to Address Common-Cause Failure Due to Latent Design Defects**
**in Digital Safety Systems"**

## Description of Changes

This branch technical position section updates the guidance previously provided in Revision 8, issued in January 2021 (Agencywide Documents Access and Management System Accession No. ML20339A647).

The purpose of this update is to implement the expanded policy in SRM-SECY-22-0076, "Expansion of Current Policy on Potential Common Cause Failures in Digital Instrumentation and Control Systems" (ML23145A181 and ML23145A182), for addressing common-cause failures in digital instrumentation and controls. The update provides guidance for the review of risk-informed diversity and defense-in-depth assessments, in addition to the existing guidance for assessments based on best estimate methods. The update also provides review guidance for design techniques or mitigating measures, other than diversity, to address the effects of a common-cause failure of digital instrumentation and controls.

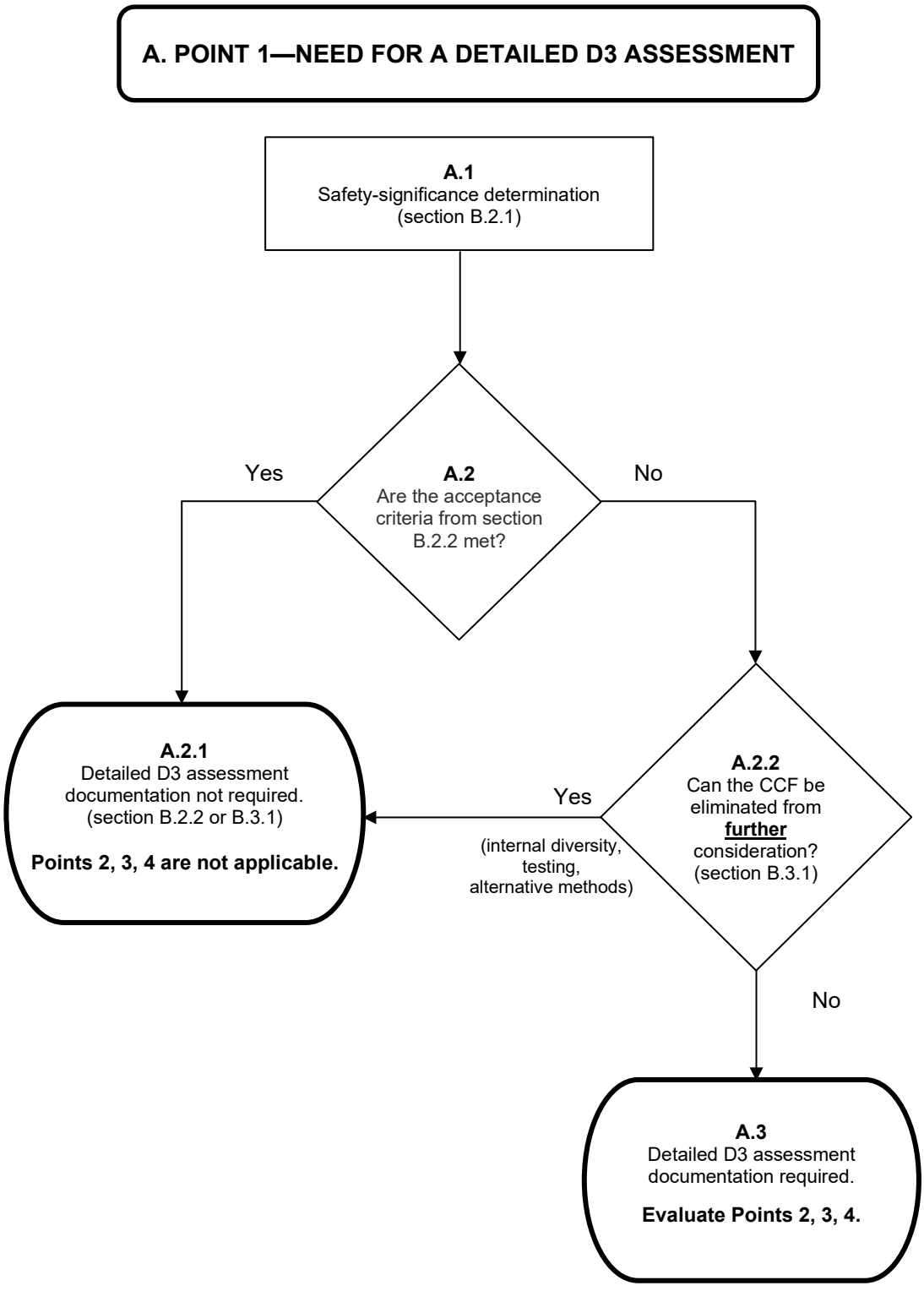


Figure 7-19-1. Point 1—Need for a Detailed D3 Assessment

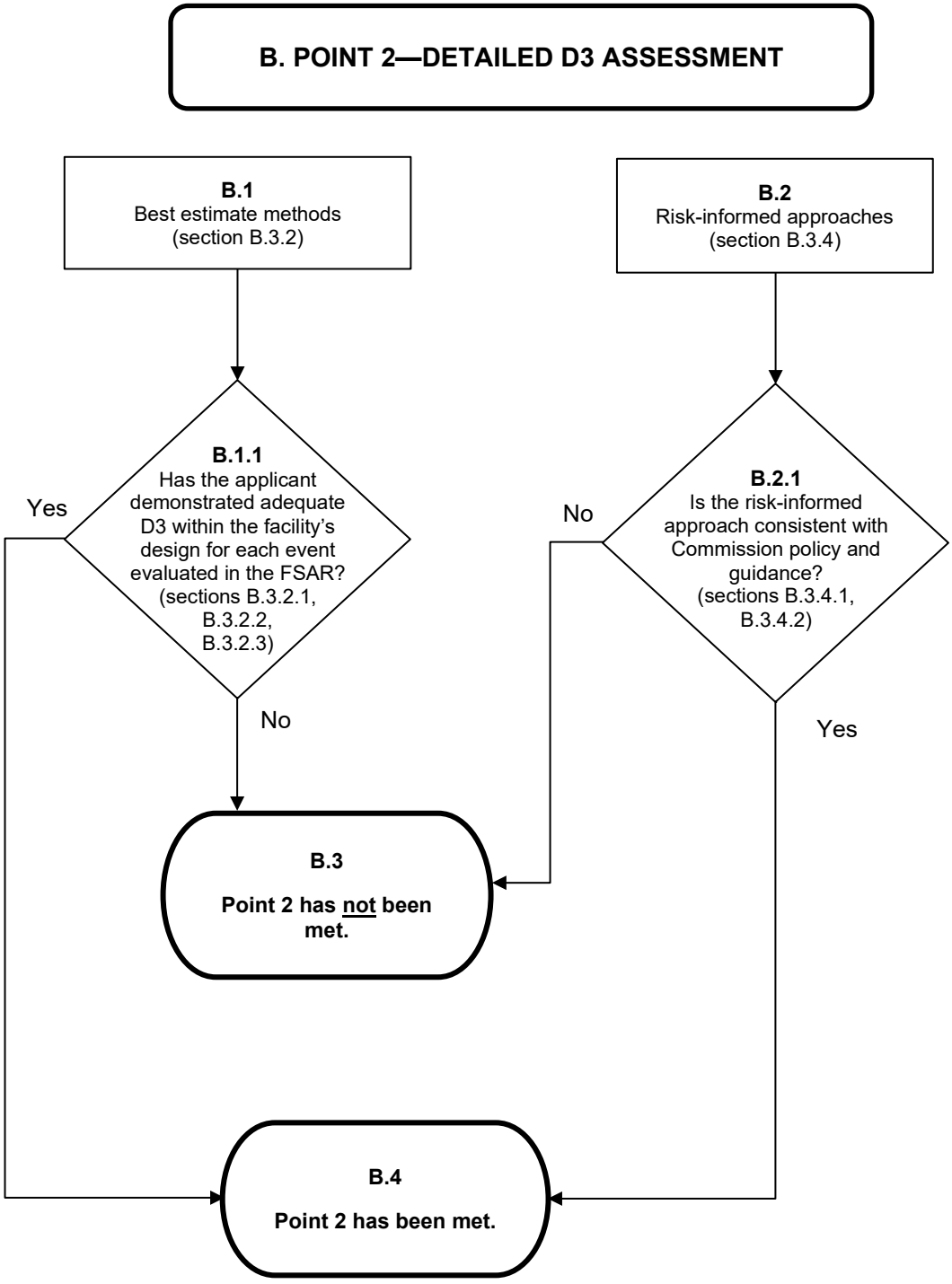


Figure 7-19-2. Point 2—Detailed Assessment

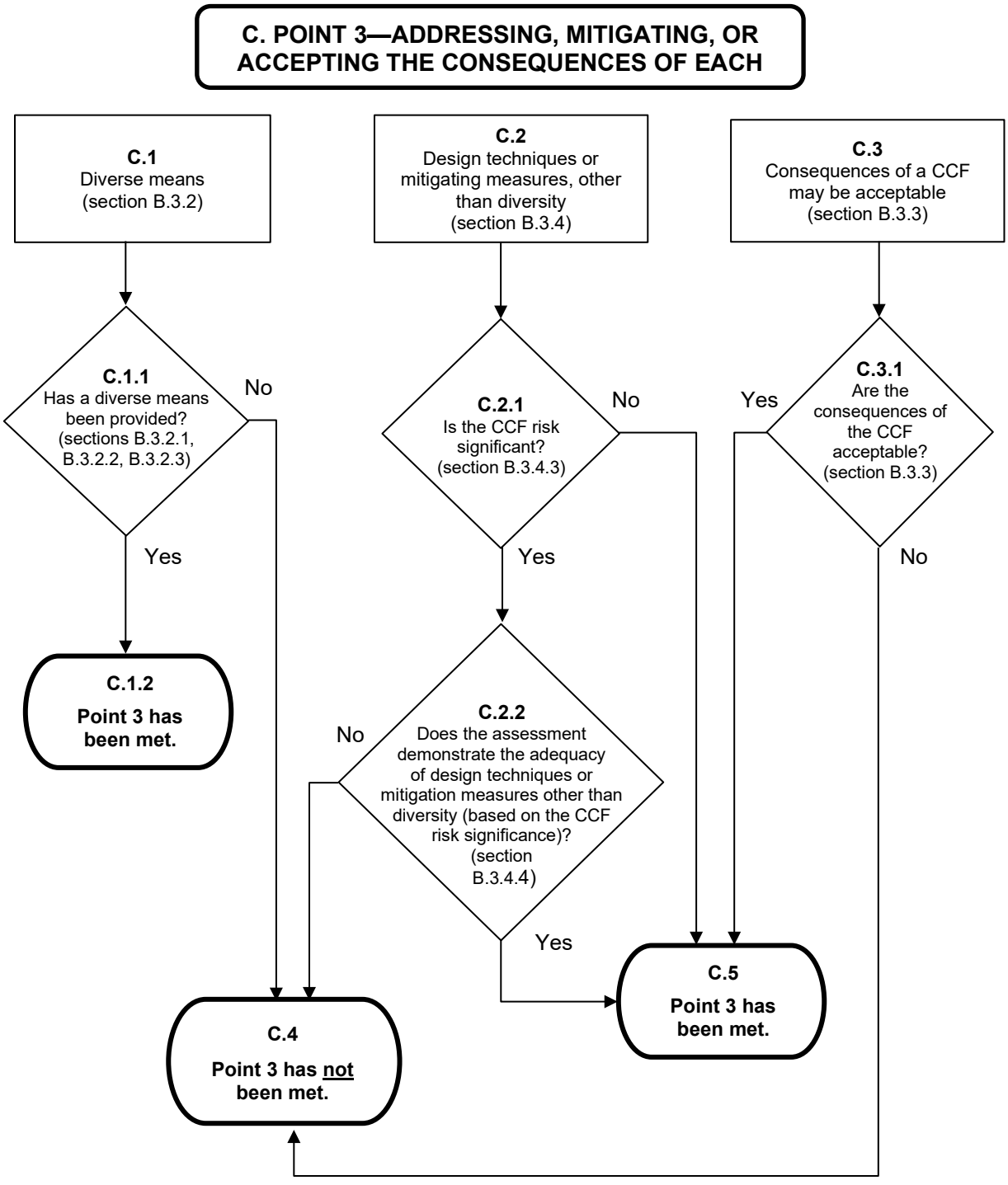


Figure 7-19-3. Point 3—Addressing, Mitigating, or Accepting the Consequences of Each CCF

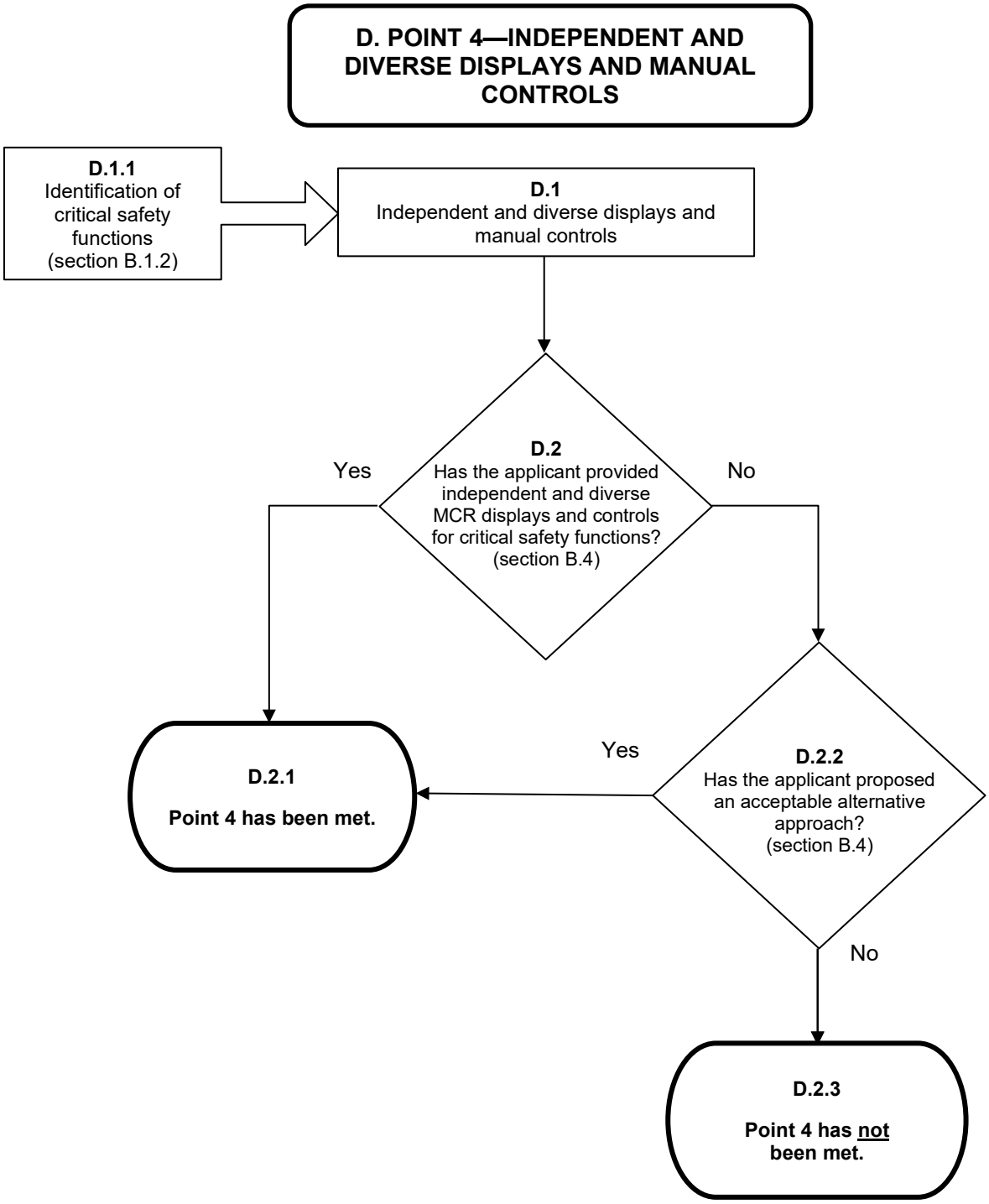


Figure 7-19-4. Point 4—Independent and Diverse Displays and Manual Controls