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 INSTRUMENTATION AND CONTROL 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

Revision 9 — May 2024

The overall objective of this branch technical position (BTP) is to provide criteria for the NRC staff's evaluation of the acceptability of the applicant's assessment of the effects of digital I&C (DI&C) system common-cause failures (CCFs).

The acceptance criteria provided in this BTP are not limited to performance characteristics of I&C systems but instead address plant performance in response to CCFs of DI&C systems. Therefore, the evaluation activities described in this BTP are not intended to be assigned exclusively to I&C technical review staff. For any given project, the activities should be coordinated and distributed among the various technical review disciplines so 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 I&C technical reviewer would be responsible for the determination of adequate independence in the design of a proposed diverse actuation system.

A. BACKGROUND

CCF has been a concern of the U.S. Nuclear Regulatory Commission (NRC) and has been addressed as part of the licensing process throughout its history (in part by defense in depth and diversity). For example, as noted in General Electric Topical Report NEDO-10189, "An Analysis of Functional Common-Mode Failure in General Electric Boiling Water Reactor Protection and Control Instrumentation," in early 1969, concern for possible effects of common-mode-type failures on plant operation—particularly in regard to nuclear safety functions—led the Atomic Energy Commission (AEC) to request the various reactor manufacturers to systematically examine their plant designs in that respect. Furthermore, in 1971 (36 FR 3255), the AEC promulgated the final version of Title 10 of the *Code of Federal Regulations* (10 CFR) Part 50, "Domestic Licensing of Production and Utilization Facilities," Appendix A, "General Design Criteria for Nuclear Power Plants," which now states the following:

> The development of these General Design Criteria is not yet complete. For example, some of the definitions need further amplification. Also, some of the specific design requirements for structures, systems, and components important to safety have not as yet been suitably defined. Their omission does not relieve any applicant from considering these matters in the design of a specific facility and satisfying the necessary safety requirements. These matters include: ...(4) *Consideration of the possibility of systematic, nonrandom, concurrent failures of redundant elements in the design of the protection systems and reactivity control systems* [*emphasis* added].

All licensed facilities are considered to have sufficient design features to address CCFs associated with their specific designs and equipment. The use of different designs, equipment, or technology may result in the need for additional design features to address the specific vulnerabilities of the different designs, equipment, or technology.

DI&C systems offer significant operational and maintenance benefits for nuclear power plants. 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., devices programmed with hardware description languages).

DI&C systems 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 fail due to a shared cause.[2] Latent design defects in the design of a DI&C system can remain undetected despite traditional design-basis development, verification, validation, and testing processes. Certain events, unexpected external stresses, or plant conditions can trigger latent design defects within redundant portions of a system designed to perform safety functions and thus lead to a systematic failure of the redundant portions.

CCFs can have two distinct 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.

In accordance with Commission direction in the staff requirements memorandum (SRM), dated July 21, 1993, on SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," dated April 2, 1993, the NRC staff considers CCFs in DI&C systems to be beyond design-basis events.[3] 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. These modifications could 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 potential for

---

1 In this BTP, the term "CCF" always refers 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 structures, systems, and components (SSCs) are similar to but distinguishable from cascading failures due to single random failures. Single failures must be addressed by meeting the principal design criteria of the facility or the criteria described in 10 CFR 50.55a(h) (i.e., the safety design criteria in Institute of Electrical and Electronics Engineers (IEEE) Std 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations," or IEEE Std 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations"). Because such failures are likely to occur during the life of the plant, the plant's design basis needs to include analysis of the possible effects (consequences) of such failures.

3 SRM-SECY-93-087 states, "The staff's position has been modified in essentially two respects: First, **inasmuch as** common mode failures are beyond design-basis events, the analysis of such events should be on a best-estimate basis…" [emphasis added]. The NRC Glossary defines "beyond design-basis accidents" as follows:

> This term is used as a technical way to discuss accident sequences that are possible but were not fully considered in the design process because they were judged to be too unlikely. (In that sense, they are considered beyond the scope of design-basis accidents that a nuclear facility must be designed and built to withstand.) As the regulatory process strives to be as thorough as possible, "beyond design-basis" accident sequences are analyzed to fully understand the capability of a design.

The design basis of a facility generally addresses certain beyond design-basis events. For example, 10 CFR 50.34, "Contents of applications; technical information," includes "(i) Mitigation of beyond-design-basis events…."

interdependencies among 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 software or software-based logic, or (3) unidentified dependencies, unintended interactions, or emergent behavior, especially when the DI&C systems are interconnected or use shared resources.

Traditionally, CCF vulnerabilities of DI&C systems have been addressed using the principles of defense in depth and diversity (D3). Under these principles, the operation of facility systems is modeled as a series of successive layers of defense (called “echelons of defense”), all 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, the extent of interconnections, and the types and use of shared resources. Generally, the design technique of independence (e.g., communication independence) is used to ensure that multiple echelons will 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 segmentation; 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.

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 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 and standards 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. The Institute of Electrical and Electronics Engineers (IEEE) standards and design criteria listed are examples of plant-specific licensing-basis items.

- IEEE 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,” together with the correction sheet dated January 30, 1995, provide criteria applicable to protection and safety systems.

- General Design Criterion (GDC) 22, “Protection system independence,” of Appendix A to 10 CFR Part 50 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.

2. Relevant Guidance

The following documents provide useful guidance in the evaluation of possible CCFs affecting DI&C systems:

- SECY-93-087, 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 staff 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 the option of not providing diverse automatic actuation of safety functions. The staff also requested that this expanded policy apply to all types of nuclear power plants.

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

- In SRM-SECY-22-0076, dated May 25, 2023, the Commission approved the staff’s recommendation in SECY-22-0076, with edits, and provided directions to the 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.

- In SRM-SECY-10-0121, dated March 2, 2011, the Commission disapproved the staff’s recommendation to modify risk guidance for new reactors described in SECY-10-0121, “Modifying the Risk-Informed Regulatory Guidance for New Reactors,” dated September 14, 2010. The SRM reaffirmed that the existing safety goals, safety performance expectations, subsidiary risk goals and associated risk guidance (such as the Commission’s Policy Statement on the Regulation of Advanced Reactors (73 FR 60612; October 14, 2008) and Regulatory Guide (RG) 1.174, “An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis”), key principles, and quantitative metrics for implementing risk-informed decision-making are sufficient for new plants.

- 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 on 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 or applicants consider cybersecurity design features, they should include measures 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 systems. (For

- example, 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 licensing-basis changes that consider engineering issues and apply 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.

- NUREG/CR-6303, “Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems,” issued December 1994, summarizes several D3 analyses performed after 1990. It presents a method for analyzing proposed DI&C systems to identify vulnerabilities to common-mode failures 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. This type of analysis is referred to as a D3 assessment in this document.

- 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.

- NUREG-2122, “Glossary of Risk-Related Terms in Support of Risk-Informed Decisionmaking,” issued November 2013, defines terms used in risk-informed activities related to commercial nuclear power plants.

3. Scope

The guidance in this BTP is intended for the NRC staff review of D3 assessments to address CCF in DI&C systems.[4] 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 is intended to provide review guidance to the NRC staff for ensuring that an application meets the policy and applicable regulations—it is not intended as guidance to applicants for developing a D3 assessment.

This BTP does not cover review criteria for single random failures and cascading failures from

[4] SRM-SECY-22-0076 uses the term “digital I&C system.”

single random failures in shared resources. 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.”

4. 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 systems 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 DI&C system—that may eliminate a potential CCF from further consideration[5]
- 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-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 CCFs in DI&C systems.

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

- a description of the overall defense-in-depth posture 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

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

- 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-22-0076, which is centered on 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., 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 logical structure of this BTP addresses the four points in SRM-SECY-22-0076, as shown in Figure 7-19-1. The following BTP sections apply to the evaluation of an application against the four points of SRM-SECY-22-0076:

- Point 1—determining 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—performing 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—addressing, mitigating, or accepting 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—providing 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 7-19-2, 7-19-3, 7-19-4, and 7-19-5 at the end of this document provide a visual aid to reviewers for 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 described 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, that is, 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. 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 a loss of offsite power, the assessment does not need to assume another concurrent design-basis event (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 will 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 of performing 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 basis that this equipment is of sufficient quality and is unlikely to be subject to the same CCF. The diverse means may already exist in the facility or may be installed in connection with the DI&C modification. For example, an anticipated transient without scram (ATWS) system may be credited as a diverse means of tripping the reactor, provided it is not vulnerable to the same CCF that could disable the safety function.

The displays and controls credited for Point 4 provide for effective manual control of critical safety functions. The same assessment performed to address the first three points may identify whether the main control room (MCR) displays and controls for manual actuation of critical safety functions are independent and diverse from the proposed DI&C system. If so, these displays and controls may be used to credit manual operator actions in Point 3 (see

section B.3.2.2). These independent and diverse displays and manual controls do not have to be safety grade or hardwired. Alternatively, the applicant may propose a different approach to Point 4 of SRM-SECY-22-0076 if the plant design provides a commensurate level of safety (see section B.4).

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 critical safety functions listed in SECY-22-0076 (i.e., reactivity control, core heat removal, reactor coolant inventory, containment isolation, and containment integrity) are examples 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 critical safety functions.

2. Safety Significance and Effects of Failure

Principle 3 of SECY-18-0090 explains 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 SRM-SECY-22-0076 states that the D3 assessment must be commensurate with the risk significance of the DI&C system, as described further below. Furthermore, Point 3 of SRM-SECY-22-0076 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.

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 reactor trip system (RTS) and engineered safety features actuation system are generally deemed more critical than those systems that perform auxiliary safety functions not directly credited in the accident analysis. Consequently, a CCF assessment for an RTS should generally be more

[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."

rigorous than, for example, a CCF assessment 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 has the potential to introduce additional dependencies and 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 application includes a clear description of the proposed DI&C system 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 a plant's defense in depth. For data communication interconnectivity, the reviewer should verify that such interconnectivity does 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 system interconnectivity and the consequences of a CCF that could affect the proper operation 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

The three safety-significance determination categories[7] below 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

[7] The safety-significance determination categories used in this BTP are consistent with SECY-18-0090.

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 but 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 Defense-in-Depth and Diversity 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 Defense in Depth and Diversity

If an SSC meets the following acceptance criteria, 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:

a. 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.

b. The SSC is not interconnected with a more safety-significant SSC.

c. 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.

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

3. Detailed Defense-in-Depth and Diversity Assessment

A D3 assessment is a systematic analysis of 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 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 affect 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.

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 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 (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 system (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.[8] 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, could 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 a spurious operation that would have unacceptable consequences. The reviewer should also consider the level of interconnection between a safety system and other systems as a potential vulnerability to be addressed in the application.[9]

---

[8] 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.

[9] See IEEE Std 603-1991.

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 the purposes of this assessment.

3.1 Means to Eliminate the Potential for Common-Cause Failures 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, (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 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 so that further evaluation is unnecessary for that portion of the SSC.

The following sections discuss each of the acceptable methods for eliminating the potential for CCFs from further consideration.

3.1.1 Use of Diversity within the Digital Instrumentation and Control System to Eliminate the Potential for Common-Cause Failures from Further Consideration

Diversity within a DI&C system constitutes the use of different techniques, schemes, features, or additions to eliminate a CCF from further consideration. If diversity is used, then each portion of the system will have 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 through the use of different technologies, algorithms, or logic; sensing devices; or actuation devices. However, diversity needs to be paired with independence from equipment performing the same function within the DI&C 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.

<u>Acceptance Criteria for Use of Diversity within the Digital Instrumentation and Control System</u>

If the following acceptance criteria are met, the reviewer should conclude that the application provides adequate information on the use of diversity within the DI&C system to eliminate the potential CCF from further consideration:

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

b. The different portions of the DI&C system 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 DI&C system do not have common or shared resources, such as power supplies, memory, bus, or communications modules, whose failure could result in a failure to perform safety functions or in adverse plant conditions that cannot be reasonably mitigated. Also, the diverse portions of the DI&C system 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 the Potential for Common-Cause Failures from Further Consideration

CCF vulnerabilities in DI&C systems 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 a DI&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 shows that all latent design defects have been identified and corrected, so that the system 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 following acceptance criteria are met, the reviewer should conclude that the application provides sufficient information on the test results and testing methodology for the DI&C system to eliminate the potential CCF from further consideration:

a. Testing covers the expected performance of the proposed DI&C system in each of its functional modes of operation and for all transitions between modes. For this purpose, testing should 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 DI&C system that accurately represents the system to be installed, guaranteeing that the DI&C 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 Failures from Further Consideration

Applicants may propose technical approaches to address CCF that this BTP does not describe (e.g., a watchdog timer not dependent on the DI&C system software that puts the actuators in the safe state may address certain CCF vulnerabilities). These approaches may consist of 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 that the method is implemented in a manner 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. Therefore, this BTP does not provide additional guidance in this regard.

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 or testing 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.

Acceptance Criteria for Use of a Proposed Alternative Approach

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 the following:

a. the identification of the CCF vulnerabilities or causes that the proposed alternative approach addresses (if these CCF vulnerabilities or causes are identified using a hazard analysis technique, then the analysis should be demonstrated to be sufficiently 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 Failures 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 DI&C system's likelihood of failure due to CCF is low enough so that current licensing assumptions will continue to be met, because the likelihood of CCF is much lower than that of other kinds of failures considered in the FSAR. This level of likelihood of CCF is referred to as "sufficiently low," and its definition compares the likelihood of failure of a proposed DI&C system to that of 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.

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

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

Second, the reviewer should consider any failure analyses used in the qualitative assessment, including information from engineering design work, such as FMEA and FTA. The reviewer should consider whether the failure analyses support the factors above and whether they demonstrate, for example, that identified potential CCFs exhibit a low likelihood of occurrence.

Acceptance Criteria for Use of Qualitative Assessment

If the following acceptance criteria 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, for SSCs of low safety significance, that the likelihood of CCF is sufficiently low:

a. The proposed DI&C system has design attributes and features that reduce the likelihood of CCFs.

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

c. The applicable operating experience collectively supports the conclusion that the proposed DI&C system 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 DI&C system 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 mitigate the impact of a postulated CCF, either by accomplishing a function that is the same as, or is different from the safety function disabled by the CCF; or by mitigating spurious operations resulting from the CCF.

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, and new diverse systems.

3.2.1 Crediting Existing Instrumentation and Control Systems

An existing reliable I&C system can be used as a diverse means either 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 I&C 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 DI&C system. If an existing I&C system is credited, then the reviewer should verify that the applicant has performed an analysis demonstrating that the credited system and the proposed DI&C system are not both vulnerable to the same CCF.

The reviewer should verify that the applicant has considered how the existing I&C system is credited in the facility's licensing basis and described in the existing I&C system's documentation (e.g., the FSAR, detailed design documents). Among other things, the reviewer should consider whether the applicant has appropriately accounted for any unique I&C system design attributes and requirements and for any potential interconnectivities, including resource sharing, with other systems. The reviewer should pay particular attention to whether there may be interconnectivities (including resource sharing) not accounted for in the LAR that could result in the existing I&C system being subject to the same CCF as the proposed DI&C system. The reviewer should verify that the application identifies all the features of the existing I&C system that are relevant to demonstrating diversity. In addition, if crediting an existing I&C system could affect the facility's existing licensing basis, then the reviewer should verify that the LAR addresses how the existing I&C system functions would be credited and justified in a revised licensing basis.

The credited existing I&C 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 existing I&C systems that are not safety related that are in continuous use (e.g., the normal control systems for the reactor coolant system inventory or the steam generator level), these systems need not meet augmented quality standards. However, if the applicant credits existing I&C 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 has 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 I&C system and other systems are adequately prioritized to maintain the overall defense-in-depth strategy and existing licensing basis. 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 I&C system has priority over the resources (e.g., operational control functions) 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 Existing I&C 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 I&C plant system as a diverse means. The existing I&C system may perform the same function as the one disabled by the postulated CCF, or it may perform a different function to compensate for or mitigate the loss of the disabled function.

a. If the diverse I&C 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.

b. Sufficient diversity exists between the diverse I&C system and the proposed DI&C 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.

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

e. If prioritization is used, the new use of the credited existing I&C system maintains the existing prioritization scheme. If the new use of the existing I&C system requires 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 needed for safety and protection are always performed over other functions.

3.2.2 Crediting Manual Operator Action[10]

When addressing Point 3 of SRM-SECY-22-0076, the applicant may credit a manual operator action as a diverse means either to accomplish a function that is the same as, or is different from the 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 NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition" (SRP), Chapter 18, "Human Factors Engineering," should show that the proposed manual operator actions are 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., unlikely to be subject to

[10] IEEE Std 279-1968, IEEE Std 279-1971, and IEEE Std 603-1991 require that certain manual controls or means of manual initiation be of the same quality as the protection or safety systems; SRM-SECY-22-0076 does not eliminate these regulatory requirements. However, other means of manual control or initiation may not need to be of the same quality.

the same CCF as) the equipment performing the same function within the DI&C system. For example, the point at which the credited manual controls are connected should be downstream of the equipment that can be adversely affected by a CCF. 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.

If the applicant has 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 DI&C system and whether the applicant has 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.

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 for manual actuation of critical safety functions (see sections B.1.2 and B.4).

Protective Actions Initiated Solely by Manual Actions

For protective actions initiated solely by manual controls, the reviewer should 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 that are 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 (i.e., unlikely to be subject to the same CCF as) the equipment performing the same function within the DI&C system.

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.

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 Instrumentation and Control System

The applicant may propose a new diverse system (e.g., a diverse actuation system) as a diverse means either of accomplishing a function that is the same as or is different from the 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 I&C 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 I&C system can function under the event conditions expected and whether it is of adequate quality.

Prioritization

If a new diverse I&C 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 I&C system share resources (e.g., priority modules), the reviewer should consider the 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 Instrumentation and Control System

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

a. If the diverse I&C 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.

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 DI&C system.

d. Resources shared by the proposed DI&C 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 Digital Instrumentation and Control System Common-Cause Failure May Be Acceptable

This section addresses applications that propose that the consequences of a residual identified CCF remain acceptable. For such applications, 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.

For each event considered 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 DI&C system are acceptable.

Acceptance Criteria for Determination of Acceptable Consequences

If the following acceptance criteria are met, the reviewer should conclude that the application shows that the consequences of potential CCFs of the proposed system are acceptable:

a. For those postulated spurious operations that have not been fully mitigated or eliminated from further consideration, the consequences of the spurious operation 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 either in radiation release exceeding 10 percent of the applicable dose guideline values, or in 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 Defense-in-Depth and Diversity 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 its risk significance.

The risk significance of a CCF is distinct from the risk significance of the DI&C systems it may affect. Point 1 of SRM-SECY-22-0076 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 DI&C system. It is possible for a system to be risk significant because of 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 SRM-SECY-22-0076, 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 a 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 a CCF beyond the increase in risk from the loss of a single safety function.

Risk significance and safety significance are different concepts. NUREG-2122 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 an application uses a risk-informed approach since the application should not overly rely on 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 an 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 verify that an application using a risk-informed approach demonstrates that 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 SRM-SECY-22-0076 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 Point 2 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 in the portions 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, as applicable, to confirm that the risk-informed approach is consistent with the Commission's policy and guidance. The following examples provide NRC staff review guidance for applications that use a risk-informed approach for modeling DI&C systems in PRA models:

- SRP Section 19.0, "Probabilistic Risk Assessment and Severe Accident Evaluation for New Reactors," provides review guidance for the design-specific PRA for a design certification and plant-specific PRA for a combined license, respectively. SRP Section 19.0 also provides guidance for reviewing DI&C system risk assessments for new reactors.

- SRP Section 19.1, "Determining the Technical Adequacy of Probabilistic Risk Assessment for Risk-Informed License Amendment Requests after Initial Fuel Load," provides review guidance for assessing the technical adequacy of a baseline PRA used to support license amendments for operating reactors, as well as LARs submitted after initial fuel load for new reactors.

- 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 PRAs used by licensees or applicants to support licensing applications.

- Design Certification / Combined License (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, provides review guidance for assessing the technical adequacy of the PRA needed for either a design certification application under 10 CFR 52.47(a)(27) or a combined license application under 10 CFR 52.79(a)(46).

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 is consistent with the established NRC policy and applicable guidance on risk-informed decision-making.

3.4.2 Modeling Common-Cause Failures

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 the hardware or software components of DI&C systems or of 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 identifies the base PRA used to

support the D3 assessment, and whether the base PRA meets the PRA acceptability guidance in RG 1.200 or equivalent guidance for new reactors such as DC/COL-ISG-028. The application may identify an approved risk-informed application that was supported by the same base PRA. The reviewer may leverage the previous risk-informed application to help determine the technical acceptability of the base PRA to support the D3 assessment. The application should justify the exclusion of any PRA hazard or operating mode from the D3 assessment. The application should also justify any changes made to the PRA model (beyond those needed to model the CCF) 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, including the use of a newly developed method, may be classified as PRA maintenance or a PRA upgrade. 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. The reviewer should confirm whether any changes made to the PRA model constitute PRA maintenance or a PRA upgrade, based on the corresponding definition in the identified guidance. SRP Section 19.2 provides 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 could 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).

Since a CCF could affect a single plant system or function or multiple plant systems or functions, considerable care should be taken in 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 Common-Cause Failures

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:

a. The application identifies the base PRA used for the risk-informed D3 assessment, 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), and 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, the following conditions are met:

   i. The DI&C system is modeled in sufficient detail to enable the licensee to evaluate the impact of the CCF on plant equipment and functions modeled in the PRA.

   ii. The modeling addresses the impact of the CCF on plant equipment in multiple systems if the DI&C system combines functions and addresses the impact of the CCF on the ability of operators to perform manual actions, and

   iii. Adequate justification is provided to show that the impact of the CCF on plant equipment, functions, and operator actions not modeled in the PRA is not risk significant.

e. For an application addressing a CCF using surrogate events, the following conditions are met:

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

   ii. Adequate justification is provided to show 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 affecting the application are identified and dispositioned following established guidance such as RG 1.200 or equivalent guidance for new reactors, as well as 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 Common-Cause Failures

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 (e.g., for a CCF associated with an upgrade from analog to digital control room annunciators), a CCF may not disable a protective function, 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 either

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 Common-Cause Failures

If the application meets the following acceptance criteria, which are to be used in conjunction with the information in the application related to 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:

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., that the probability of failure of the surrogate events is 1) and the application describes the baseline risk used to determine the increase in risk (e.g., the basis for the nominal failure probability for the CCF used in the baseline model is 0, meaning 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 assumes a conservative value less than 1 for the probability of the CCF, the following conditions are met:

    i. The application includes a technical basis that demonstrates that an adequate level of defense in depth is provided for the conservative probability less than 1.

    ii. The application assesses the impact of this assumption on PRA uncertainty and determines whether it is a key assumption. The application also assesses the impact of the assumption on 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 of operators to perform manual actions affected by the CCF.

The following acceptance criteria, which are to be used in conjunction with the information in the application related to 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 1×10^{-6}/year.

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

3.4.4 Determining Appropriate Means to Address Common-Cause Failures

Point 3 of SRM-SECY-22-0076 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. Point 3 concludes by stating that, 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.

For risk-significant CCFs, 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 than for 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 Appropriate Means to Address Common-Cause Failures

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), then 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 CCF vulnerabilities or causes are identified using a hazard analysis technique, then the analysis should be demonstrated to be sufficiently correct and complete.

b. The application describes how the applicant addressed the CCF vulnerabilities or causes and any potential spurious operations, including any conditions or limitations. This description includes supporting information and reasoning.

c. The application includes a technical basis explaining how the applicant addressed the identified CCF vulnerabilities or causes and will prevent or mitigate their effects. The technical basis also explains how the effectiveness of the methods used for prevention or mitigation will be demonstrated.

If a postulated CCF is risk significant and the application does not demonstrate the adequacy of design techniques, prevention measures, or mitigation measures, then the diverse means provided should be reviewed using the guidance in Section B.3.2.

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

Point 4 of SRM-SECY-22-0076 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 for monitoring of parameters that support the safety functions. Section B.1.2 provides information on critical safety functions. Point 4 also states that the applicant may alternatively propose a different approach to this point in SRM-SECY-22-0076 if the plant design has a commensurate level of safety.

The reviewer should verify that the 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 could be adversely affected by a CCF.

Point 4 specifies that if the independent and diverse MCR displays and manual controls provided to meet Point 4 are not vulnerable to the same CCF as the proposed DI&C system, then the applicant may credit them as diverse means under Point 3 to address the loss of a safety function due to a CCF (see section B.3.2.2). 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, provided they meet the acceptance criteria described below or the application includes appropriate justification.

Acceptance Criteria

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

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

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

c. The proposed manual operator actions are prescribed by licensee-approved plant procedures, and operators are 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.

f. The displays and controls are independent and diverse from (i.e., unlikely to be subject to the same CCF as) the equipment performing the same functions within the proposed DI&C systems. These displays and controls are not adversely affected by postulated CCFs that could disable the corresponding functions within the proposed DI&C systems.

For applications that propose a different approach for meeting Point 4, acceptance criteria a, c, e, and f above are generally applicable regardless of the location of the equipment performing specific critical safety functions. These criteria are likely to be relevant to most applications. If an application proposes a different approach that does not meet all of the acceptance criteria above (i.e., items a–f), the reviewer should determine whether the application contains appropriate justification to show that the plant design yields a level of safety commensurate with that provided by ensuring that operators' ability to actuate the applicable critical safety functions and monitor and control the related parameters is maintained.

5. Information for Interdisciplinary NRC Staff Review

In addition to conducting the review described in the preceding sections, the I&C technical reviewer should also work with NRC staff in other disciplines to identify other areas that may be affected by CCFs. The I&C 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 a function that is the same as or different from the safety function disabled by a postulated CCF, for any CCFs not eliminated from further consideration using design attributes; also, the information provided to demonstrate the effectiveness of any diverse means credited to mitigate the potential CCF, including the results of HFE analysis for any manual operator actions used as 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 analyses demonstrating that the consequences of the CCFs 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

- 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 I&C technical reviewer should use the acceptance criteria 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 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 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 include a basis demonstrating that the different function provides 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 has 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. U.S. Nuclear Regulatory Commission (NRC), NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition," Section 7.1-T, "Table 7-1 Regulatory Requirements, Acceptance Criteria, and Guidelines for Instrumentation and Control Systems Important to Safety" (Agencywide Documents Access and Management System Accession No. ML16020A103).

2. NRC, Regulatory Guide (RG) 1.70, Revision 3, "Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants: LWR Edition," November 1978 (ML011340122).

3. Institute of Electrical and Electronics Engineers (IEEE) Std 279-1968, "Proposed IEEE Criteria for Nuclear Power Plant Protection Systems," Piscataway, NJ, August 1968.

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

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

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

7. NRC, RG 1.233, Revision 0, "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," June 2020 (ML20091L698).

8. NRC, RG 1.62, Revision 1, “Manual Initiation of Protective Actions,” June 2010 (ML092530559).

9. NRC, RG 1.53, Revision 2, “Application of the Single-Failure Criterion to Safety Systems,” November 2003 (ML033220006).

10. NRC, RG 1.152, Revision 4, “Criteria for Programmable Digital Device in Safety-Related Systems of Nuclear Power Plants,” July 2023 (ML23054A463).

11. NRC, RG 1.174, Revision 3, “An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis,” January 2018 (ML17317A256).

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

13. NRC, NUREG-0800, Section 19.2, “Review of Risk Information Used to Support Permanent Plant-Specific Changes to the Licensing Basis: General Guidance,” June 2007 (ML071700658).

14. 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).

15. NRC, NUREG-0800, Chapter 18, “Human Factors Engineering,” Revision 3, December 2016 (ML16125A114).

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

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

18. 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 (ML003708056).

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

20. 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).

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

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

23. NRC, RG 1.200, Revision 4, “Acceptability of Probabilistic Risk Assessment Results for Risk-Informed Activities,” February 2017 (ML16056A338).

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

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

26. 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).

27. 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).

28. NRC, SECY-10-0121, “Modifying the Risk-Informed Regulatory Guidance for New Reactors,” September 14, 2010 (ML102230076).

29. NRC, SRM-SECY-10-0121, “Staff Requirements – SECY-10-0121 – Modifying the Risk-Informed Regulatory Guidance for New Reactors,” March 2, 2011 (ML110610166).

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

31. General Electric, Topical Report NEDO-10189, “An Analysis of Functional Common-Mode Failure in General Electric Boiling Water Reactor Protection And Control Instrumentation,” July 1970 (ML18151A025).

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.

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, Revision 9,
GUIDANCE FOR EVALUATION OF DEFENSE IN DEPTH AND DIVERSITY TO ADDRESS COMMON-CAUSE FAILURE DUE TO LATENT DESIGN DEFECTS IN DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS

Description of Changes

This branch technical position section updates the guidance previously provided in Revision 8, issued 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, “Staff Requirements—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 defense-in-depth and diversity 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 common-cause failures in digital instrumentation and controls.

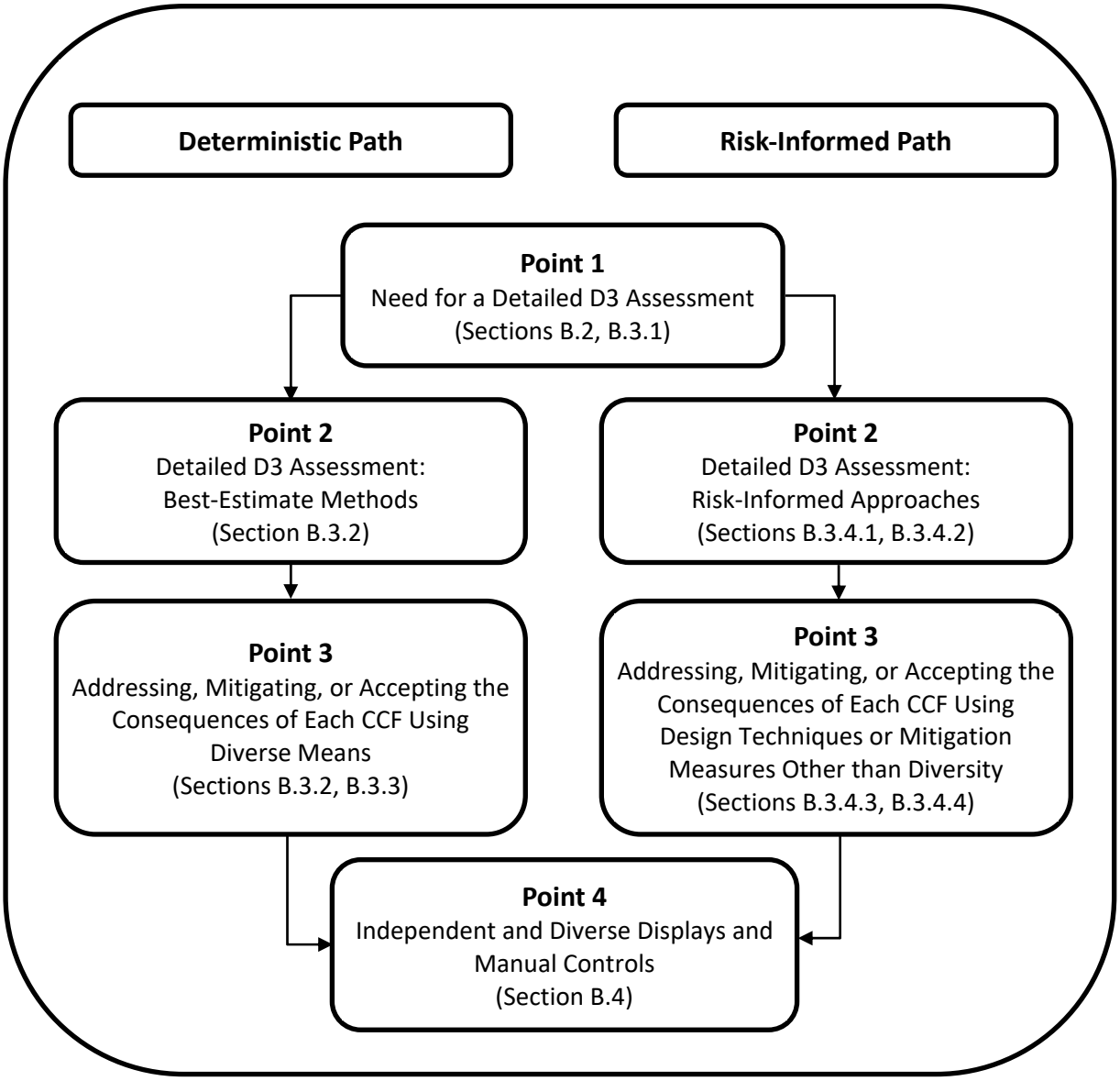

Figure 7-19-1 Four points of SRM-SECY-22-0076 and applicable BTP 7-19 sections

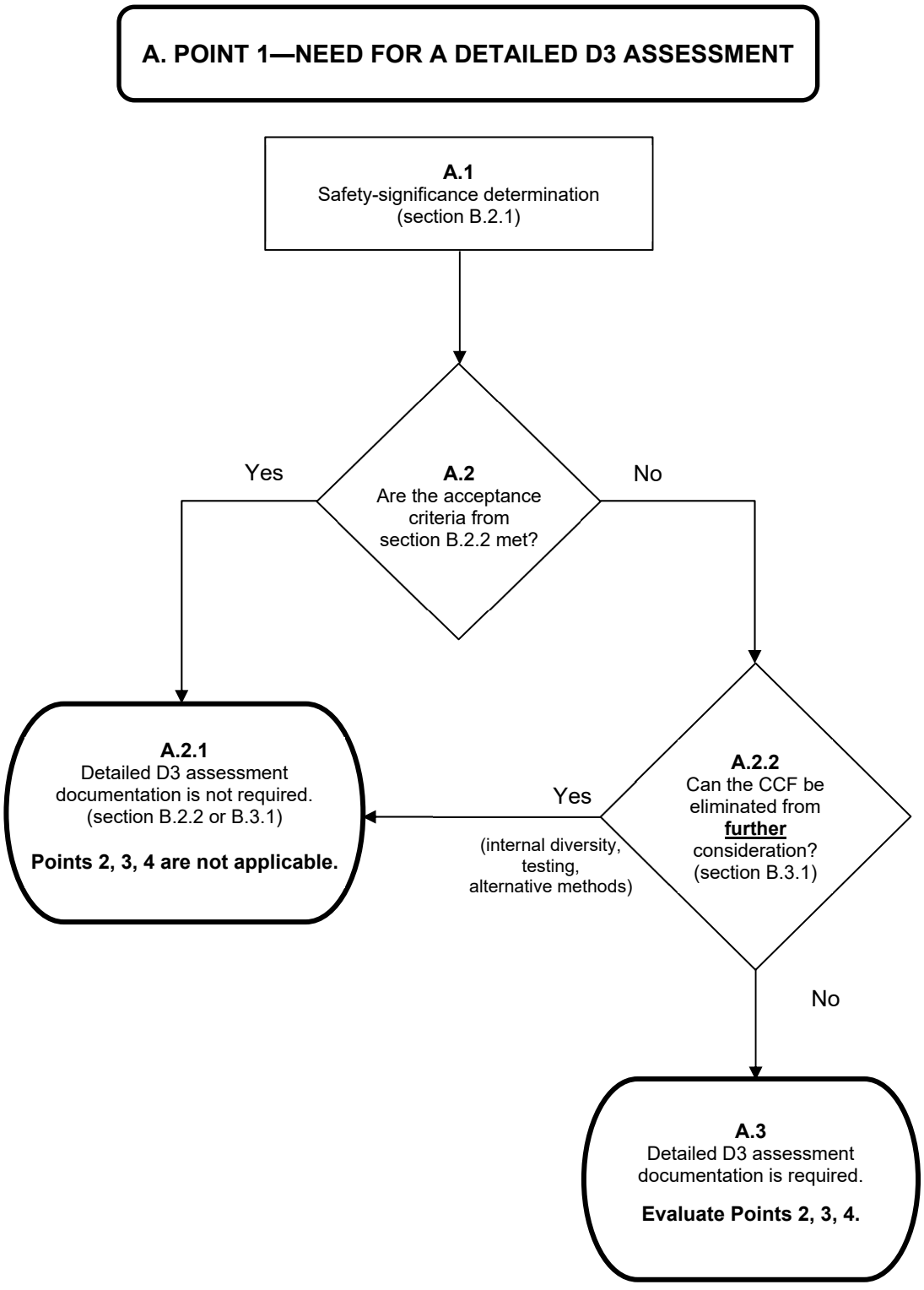

Figure 7-19-2 Point 1—need for a detailed D3 assessment

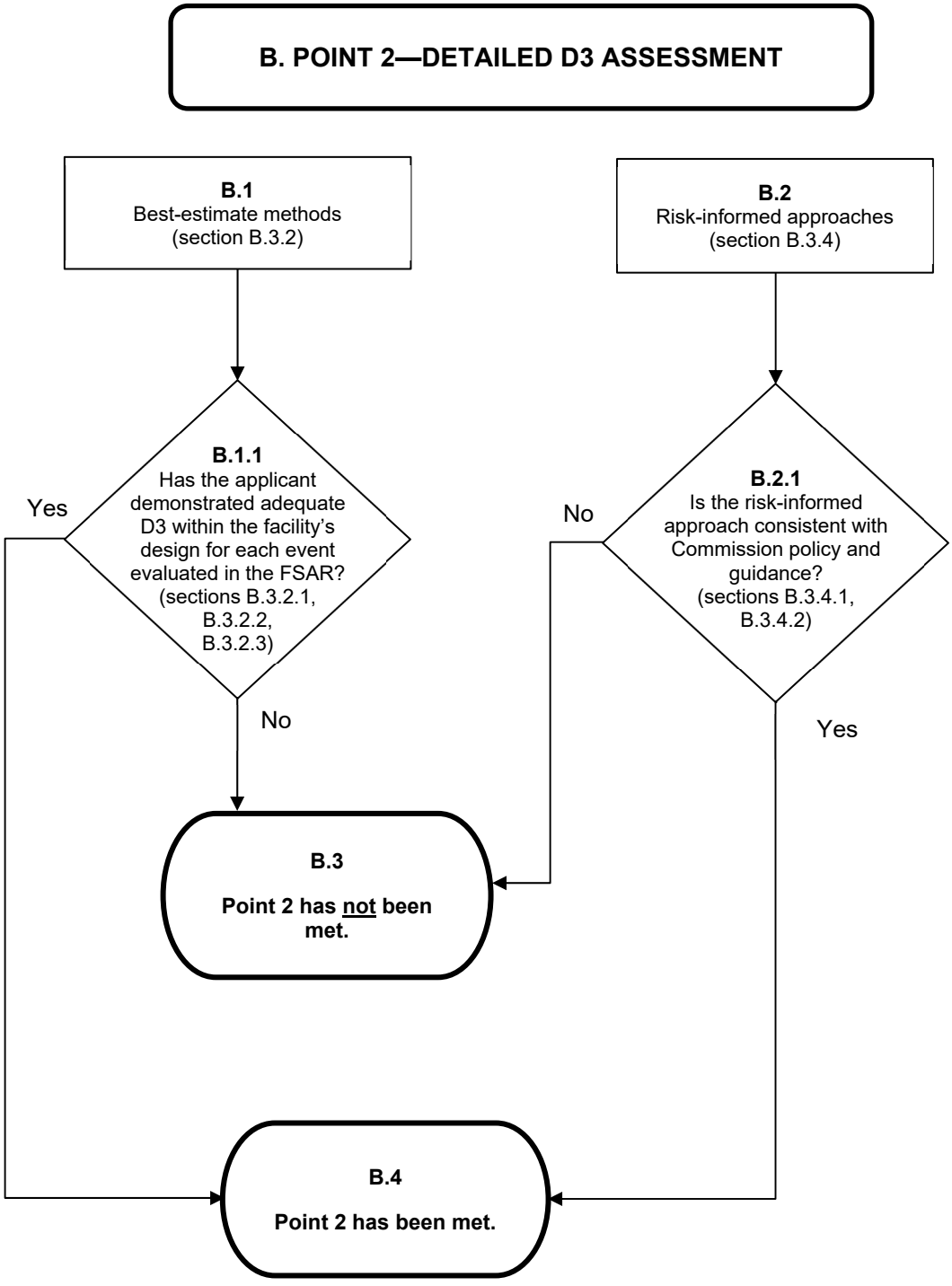

Figure 7-19-3 Point 2—detailed D3 assessment

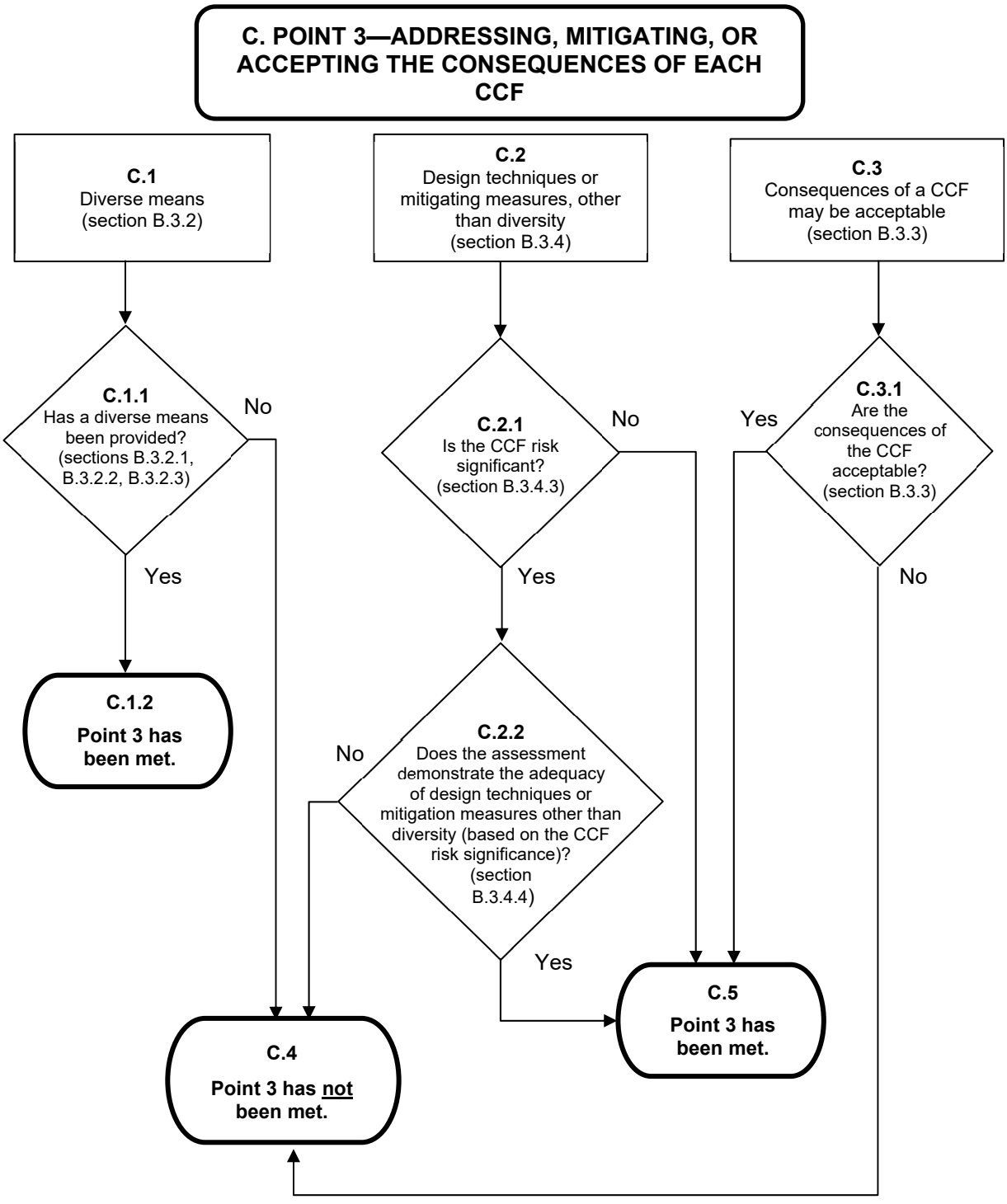

Figure 7-19-4 Point 3—addressing, mitigating, or accepting the consequences of each CCF

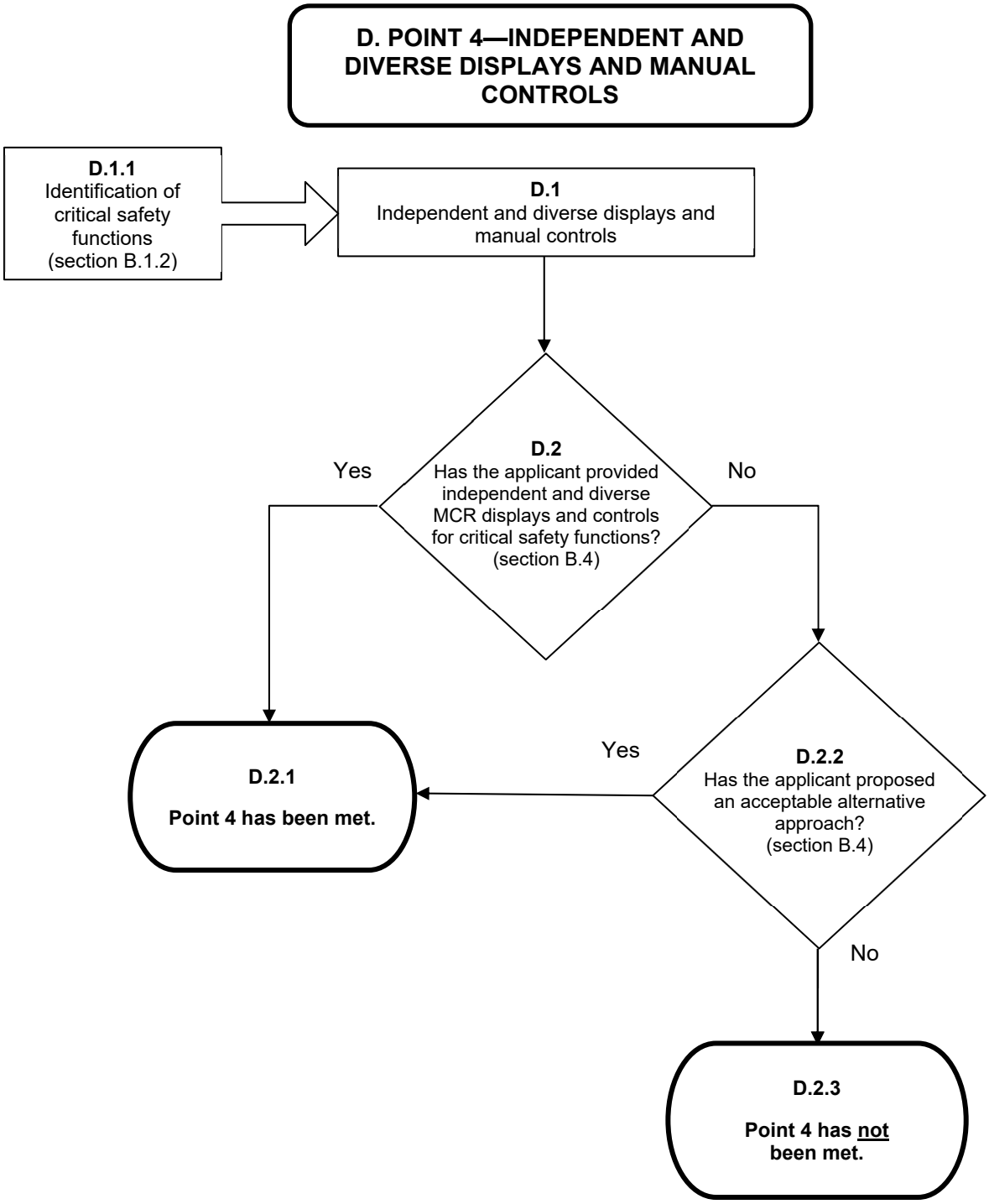

Figure 7-19-5 Point 4—independent and diverse displays and manual controls

SUBJECT: FINAL REVISION TO 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 INSTRUMENTATION AND CONTROL SYSTEMS" DATED APRIL 25, 2024

DISTRIBUTION:

PUBLIC	JPaige, NRR
Croque-Cruz, NRR	FSacko, NRR
MMarshall, NRR	MMcConnell, NRR
UShoop, NRR	DTaneja, NRR
MFranovich, NRR	LRamadan, NRR
TMartinezNavedo, NRR	DRahn, NRR
EBenner, NRR	WRoggenbrodt, NRR
RidsNrrDorlLlpb	SAlferink, NRR
RidsNrrDorl	CCheung, NRR
RidsNrrDra	GBlasRodriguez, NRR
RidsNrrDex	NCartre, NRR
RidsOgcMailCenter Resource	MLi, NRR
RidsACRS_MailCTR	SDarbali, NRR
SVasavada, NRR	JAshcraft, NRR

ADAMS Accession Nos.:
ML24005A119 (Package)
ML24005A077 (Final Review Plan)
ML24005A108 (FRN)
ML24005A115 (Response to Public Comments)

OFFICE	NRR/DORL/LPMB/PM	NRR/DORL/LA	NRR/DORL/LPL1/PM	NRR/DEX/EICB/BC
NAME	CRoque-Cruz	ABaxter	MMarshall	FSacko (A)
DATE	1/4/2024	1/9/2024	1/9//2024	1/12/2024
OFFICE	NRR/DEX/ELTB/BC	NRR/DRA/APLC/BC	NRR/DEX/D	NRR/DRA/D
NAME	JPaige	SVasavada	EBenner	MFranovich
DATE	1/12/2024	1/12/2024	1/18/2024	1/18/2024
OFFICE	QTE	OCIO	OGC - NLO	NRR/DORL/LPMB/BC
NAME	JDougherty	DCullison	DRoth	UShoop
DATE	2/2/2024	3/13/2024	3/1/2024	4/25/2024

OFFICIAL RECORD COPY