U.S. NUCLEAR REGULATORY COMMISSION

STANDARD REVIEW PLAN

BRANCH TECHNICAL POSITION 7-19

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

REVIEW RESPONSIBILITIES

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

Secondary – Organizations responsible for the review of reactor and containment systems and organizations responsible for the review of human factors engineering (HFE)

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

Revision 8 – January 2021

Power Plants: LWR Edition" (SRP), Table 7-1, "Regulatory Requirements, Acceptance Criteria, and Guidelines for Instrumentation and Control Systems Important to Safety" (Table 7-1). This BTP does include the associated year in references to industry standards incorporated by reference into regulations (Institute of Electrical and Electronics Engineers (IEEE) Standard (Std) 279-1968, IEEE Std 279-1971, and IEEE Std 603-1991), as well as industry standards that are not endorsed by the agency. Users should consult Table 7-1 to ensure that reviews apply the appropriate RGs and endorsed industry standards.

A. BACKGROUND

Digital technology offers significant operational and maintenance benefits for I&C systems of nuclear power plants (NPPs). Digital instrumentation and control (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,[1] and logic developed from software-based development systems (e.g., hardware description language programmed devices).

DI&C systems or components are vulnerable to common-cause failures (CCFs) due to latent design defects in active hardware components, software, or software-based logic.[2] A CCF occurs when multiple (usually identical) systems or components fail due to a shared cause.[3] Latent design defects are errors in the design of the DI&C system or component that can remain undetected despite rigorous design-basis development, verification, validation, and testing processes. Certain events, unexpected external stresses, or plant conditions can trigger latent design defects within redundant portions (e.g., safety divisions) of a system designed to perform safety functions and thus lead to a systematic failure.

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

In accordance with Commission direction in the staff requirements memorandum (SRM) on SECY-93-087, "SECY-93-087—Policy, Technical, and Licensing Issues Pertaining to

---

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

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

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

Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," dated July 21, 1993, the staff considers CCF in DI&C systems to be a beyond-design-basis event. 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 systems can integrate design functions that were previously located in separate and dedicated analog systems. For example, formerly discrete systems (e.g., the reactor trip system (RTS) and the engineered safety feature actuation system (ESFAS)) can be combined into a single DI&C protection system. Also, DI&C systems can share resources, such as communications, networks, controllers, power supplies, or multifunction display and control stations. The integrability of DI&C systems makes it more challenging to identify and evaluate potential consequences of a postulated CCF.

Generally, except in a few structures, systems, and components (SSCs) with very simple designs, DI&C systems containing software or logic cannot be fully tested, nor can their failure modes be completely predicted, because software has too many potential failure modes for deterministic predictions to be feasible. Therefore, DI&C systems may be vulnerable to CCF if either (1) identical system designs and identical copies of the software or software-based logic are present in redundant divisions of the systems, or (2) the DI&C systems are integrated and interconnected (e.g., they use shared resources).

CCF vulnerabilities of DI&C systems or components are addressed using the principles of defense in depth. Under these principles, the operation of facility systems is modeled as a series of successive layers of defense (called "echelons of defense"), each of which would need to be defeated for a CCF to result in unacceptable harm to public health and safety. A CCF could affect multiple echelons of defense and redundant divisions, depending upon, for example, the system architecture, level of integration, and type and use of shared resources. NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems," issued December 1994, describes defense in depth for NPPs. For example, Section 2.2 of NUREG/CR-6303 identifies the normal reactor control systems, the RTS, the ESFAS, and the reactor monitoring and indication systems as individual echelons of defense.

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, or withstand or cope with the effects of a CCF. Traditional design techniques such as redundancy, independence, and diversity ensure that the architecture provides the basic framework and structure for maintaining defense in depth. Other design features can also contribute to overall defense in depth. Such features include predictable real-time (deterministic) processing, automated self-test provisions, and measures to control access to physical, electronic, and software-based elements that, if tampered with or corrupted, could cause adverse plant consequences. The following documents provide staff guidance for evaluating these features:

- SRP Appendix 7.0-A, "Review Process for Digital Instrumentation and Control Systems," and BTP 7-21, "Guidance on Digital Computer Real-Time Performance," provide

guidance on real-time deterministic processing.

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

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

- RG 5.71, "Cyber Security Programs for Nuclear Facilities," provides guidance on protecting digital computers and communication systems and networks against cyberattacks.

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

Over the years, the U.S. Nuclear Regulatory Commission (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 staff has evaluated several different solutions that successfully address CCF vulnerabilities. Consequently, the staff recognizes that there may be no single solution that applies to all DI&C systems.

1. Regulatory Basis

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

- For NPPs with construction permits (CPs) issued before January 1, 1971, Title 10 of the *Code of Federal Regulations* (10 CFR) 50.55a(h) requires protection systems to be consistent with the plant-specific licensing basis or to comply with IEEE Std 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," and with the IEEE Std 603-1991 correction sheet dated January 30, 1995.

- For NPPs with CPs issued between January 1, 1971, and May 13, 1999, 10 CFR 50.55a(h) requires protection systems to comply with IEEE Std 279-1968, "Proposed IEEE Criteria for Nuclear Power Plant Protection Systems"; IEEE Std 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations"; or IEEE Std 603-1991 and the correction sheet dated January 30, 1995.

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

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

  > The protection system shall be designed to assure that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function, or shall be demonstrated to be acceptable on some other defined basis. Design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protection function.

- GDC 24, “Separation of protection and control systems,” of Appendix A to 10 CFR Part 50 states in part that “interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired.”

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

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

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

- The regulations in 10 CFR Part 52, “Licenses, certifications, and approvals for nuclear power plants,” govern applications for early site permits, DCs, COLs, SDAs, and manufacturing licenses (MLs) for nuclear power facilities.

- The regulations in 10 CFR Part 100, “Reactor site criteria,” Subpart A, “Evaluation Factors for Stationary Power Reactor Site Applications Before January 10, 1997 and for

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

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

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

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

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

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

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

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

2. Relevant Guidance

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

- NUREG/CR-6303 summarizes several diversity and defense-in-depth (D3) analyses performed after 1990. It presents a method for analyzing proposed DI&C systems to identify vulnerabilities to common-mode failures[4] 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

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

determines what portions of a design need additional D3 measures to address such failures.

- NUREG/CR-7007, "Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems," issued December 2008, 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.

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

- SECY-18-0090, "Plan for Addressing 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.

- Generic Letter (GL) 85-06, "Quality Assurance Guidance for ATWS Equipment That is Not Safety-Related," dated April 16, 1985, provides quality assurance guidance for anticipated transient without scram (ATWS) equipment that is not safety related (NSR). GL 85-06 describes methods that may be used to establish quality assurance measures for equipment that is NSR and credited for providing the diverse means to mitigate potential CCFs.

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

- Regulatory Issue Summary (RIS) 2002-22, Supplement 1, "Clarification on Endorsement of Nuclear Energy Institute Guidance in Designing Digital Upgrades in Instrumentation and Control Systems," dated May 31, 2018, clarifies guidance for preparing and documenting qualitative assessments that can be used to evaluate the likelihood of failure of a proposed DI&C system or component modification.

- SRP Table 7-1, "Regulatory Requirements, Acceptance Criteria, and Guidelines for Instrumentation and Control Systems Important to Safety."

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

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

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

- DI&C-ISG-04, “Highly-Integrated Control Rooms—Communications Issues (HICRc),” provides interim staff guidance (ISG) for addressing interactions among safety divisions and between safety-related equipment and equipment that is not safety related.

3. Scope

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

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

- proposed design attributes—such as the use of diverse equipment, testing, or NRC-approved alternative methods, including defensive measures, in the design of a system or component—that may eliminate a potential CCF from further consideration[5]

- an applicant’s use of diverse external equipment, including manual controls and displays, to mitigate a potential CCF, as well as other measures to ensure conformance

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

with the NRC's position on addressing CCFs in DI&C systems as specified in SRM-SECY-93-087 and SECY-18-0090

This BTP also addresses review of the applicant's assessment of vulnerabilities to a CCF that can cause a spurious operation. It provides the staff with guidance for evaluating applicant analyses of a proposed modification'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 staff's evaluation of the acceptability of the applicant's D3 assessment of proposed DI&C systems.[6]

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

- a description of the overall defense-in-depth posture of plant control and protection systems adequate to protect the plant from the effects of CCFs if they were to occur
- identification and documentation of vulnerabilities to CCF
- a documented basis for any safety-significance determinations used in the application
- a failure analysis for any SSCs excluded from a D3 assessment
- a description of any D3 assessment, including the following:
  - an evaluation of vulnerabilities to a CCF, and any means used to eliminate the potential CCF from further consideration
  - 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 the consequences of the residual CCF remain acceptable

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,

[6] The review acceptance criteria in this BTP are structured as guidance to the NRC staff, so that the staff may make findings upon determining certain specified facts. The facts specified in the review acceptance criteria are not requirements, and an applicant need not establish them but may employ different facts to support the application.

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.

1.1 Four-Point Common-Cause Failure Position and Discussion

The foundation of BTP 7-19 is the NRC position on D3 from SRM-SECY-93-087, which consists of the four points quoted below:

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

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

3. If a postulated common-mode failure could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common-mode failure, shall be required to perform either the same function or a different function. The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions. [Emphasis in original.]

4. A set of displays and controls located in the main control room shall be provided for manual, system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. The displays and controls shall be independent and diverse from the safety computer system identified in items 1 and 3 above.[7]

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 or component. Section B.2 provides guidance for reviewing an applicant's safety-significance determinations, if any are used, and Section B.3.1 contains guidance for reviewing an applicant's use of those determinations in the D3 assessment. Section B.2 also covers the review of an applicant's determination that a D3 assessment is not necessary, based on a failure analysis.

Point 2 uses the term "best estimate methods," but this term is somewhat out of date; the same

[7] While SRM-SECY-93-087 uses the terms "safety" and "non-safety," from the context it is clear that these terms refer to safety-related and NSR SSCs, respectively.

methods are now typically described as methods that use “realistic assumptions,” which are defined as the initial plant conditions corresponding to the onset of the event being analyzed. Point 2 also includes acceptance criteria 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 methods using realistic assumptions identified in point 2, the 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 D3 assessment independently. For example, if the initiating event is the loss of offsite power, the assessment does not need to assume another concurrent DBE.

If the D3 assessment shows that a postulated CCF could disable a safety function, then point 3 directs that a diverse means be provided to perform that safety function or a different function. The diverse means may already exist in the facility or may be installed in connection with the DI&C modification. The diverse means may comprise NSR equipment, together with a documented basis that this equipment is of sufficient quality and is not vulnerable to the same CCF. Methods for demonstrating sufficient quality include application of the alternative treatment provided in 10 CFR 50.69(d)[8] and quality controls or measures developed in accordance with GL 85-06. SECY-18-0090 clarifies that either automatic or manual actuation within an acceptable time frame is a permissible diverse means of actuation. If the D3 assessment demonstrates that a possible CCF can be reasonably mitigated by other means (e.g., using other installed systems), a diverse means that performs the same or a different function may not be needed. For example, an ATWS system may be credited as the diverse means of tripping the reactor, provided it is not vulnerable to the same CCF that could disable the safety function.

If a diverse means is part of a safety-related system, it is then subject to the divisional independence requirements in IEEE Std 603-1991, Clause 5.6.1, which is incorporated by reference into 10 CFR 50.55a, “Codes and standards.” If the diverse means is NSR, then the requirements in IEEE Std 603-1991, Clause 5.6.3, for separation and independence between safety-related systems and NSR systems apply.

---

[8] While required for implementing 10 CFR 50.69, the quality assurance measures called for by 10 CFR 50.69(d) are not required for the equipment comprising the diverse means, but they can serve as guidance for assessing the quality of that equipment.

Point 4 directs the inclusion of a set of displays and manual controls in the main control room (MCR) that is independent of and diverse from the "safety computer system" discussed in points 1 and 3.[9] The reviewer should determine whether this set of displays and manual controls provides for divisional independence as applicable to the specific design implementation. Depending on the design, these displays and controls should provide manual system- or division-level actuation and control of equipment to manage the "critical safety functions" (see Section B.1.2).[10]

Furthermore, if not vulnerable to the same CCF as the proposed safety-related DI&C system, some of the displays and manual controls from point 4 may be credited as all or part of the diverse means provided to address point 3. The point 4 phrase "safety computer system identified in items 1 and 3" refers to a safety-related DI&C system that is credited for mitigating an AOO or PA in the accident analysis. Typically, the automatic safety-related I&C system is credited, but for some events, manual safety-related controls are credited.

1.2 Critical Safety Functions

SECY-93-0087 identified the following critical safety functions to be managed from the MCR in accordance with point 4:

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

Other safety functions an applicant identifies in the SAR may not always be "critical safety functions" in the terminology of SRM-SECY-93-087. NUREG-0737, Supplement 1, "Clarification of TMI Action Plan Requirements: Requirements for Emergency Response Capability," issued January 1983, provides additional guidance on identifying critical safety functions.

2. Safety Significance and Effects of Failure

This section provides guidance to reviewers on implementing Principle 3 in SECY-18-0090, which explains that a D3 assessment should be "commensurate with the safety significance of the system" and "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." Specifically, this section provides guidance on how to evaluate the relative safety significance of the functions performed by an SSC and how to evaluate an

---

9 While SRM-SECY-93-087 uses the terms "safety" and "non-safety," these terms in context refer to safety-related and NSR SSCs, respectively.

10 SECY-18-0090 did not elaborate on point 4.

application that does not include a D3 assessment for a low-safety-significant SSC, 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 to detect the onset of adverse reactor conditions, trip the reactor, and quickly reach a safe, stable state, systems that perform protection functions (e.g., RTS and ESFAS) are deemed more critical than those that perform auxiliary safety functions that are not directly credited in the Chapter 15 analysis in the FSAR. Consequently, a CCF assessment for an RTS should be more rigorous than one for a safety-related MCR heating, ventilation, and air conditioning (HVAC) chiller. While the HVAC chiller is a safety-related system, maintaining a certain temperature and humidity in the MCR to allow equipment and personnel to operate properly, a failure of this system is not as significant as an RTS failure because personnel have operating procedures or diverse means to control MCR temperature and humidity and can shut down the plant for this purpose if necessary. Therefore, the reviewer should evaluate the applicant's safety-significance determination for the SSC.

The reviewer should consider whether the applicant used risk insights from site-specific probabilistic risk assessments (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 Integration and Interconnectivity

System integration and interconnectivity can introduce additional CCF vulnerabilities. If there is integration (e.g., through combined design functions, shared resources, or digital interconnectivity), the system should be assessed using the methods appropriate for the highest safety-significance SSC that is integrated or interconnected. The reviewer should consider whether the applicant included a clear description of the proposed DI&C system or component that identifies (1) shared resources, (2) interconnection with other systems, and (3) whether the modification could reduce the redundancy, diversity, separation, or independence of systems described in the facility's SAR. Reductions in independence, separation, diversity, or redundancy can adversely affect the defense-in-depth of a plant.

The reviewer should also determine whether the assessment of the most safety significant SSCs considers the vulnerability to CCF resulting from failures within the integrated or interconnected system and the consequences of a CCF that could affect the proper operations of the integrated or interconnected systems. For example, a digital protection system may include controllers for performing reactor trip and engineered safety feature (ESF) logic, as well as safety control functions (e.g., auxiliary feedwater level control). If the reactor trip or ESF initiation signal in such a system reaches the final actuation device only through the equipment

that performs safety control functions, then the reviewer should determine whether all the SSCs in that pathway have been assigned to the highest safety significant SSC category. In this example, the reviewer should determine whether the D3 assessment for these interconnected or integrated systems meets the criteria in Sections B.3.1–B.3.3 for D3 assessments of high safety-significant SSCs.

Acceptance Criteria for Safety-Significance Determinations:

NRC technical reviewers should find an applicant's safety-significance determination acceptable if it reasonably conforms 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 staff should review these on a case-by-case basis. The following acceptance criteria applies:

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

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

- They are credited in the FSAR to perform design functions that contribute significantly to plant safety.
- They are relied upon to initiate and complete control actions essential to maintaining plant parameters within acceptable limits established for a DBE, or to maintaining the plant in a safe state after it has reached safe shutdown.
- Their failure could directly lead to accident conditions that may have unacceptable consequences (e.g., exceeding siting dose guidelines for a DBE) 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.

For SSCs in this category, GDC 22 requires functional diversity, to the extent practical.

b. lower safety significance: safety-related SSCs that do not perform safety-significant functions, and NSR SSCs 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 an NSR design function 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).

- Applicable GDCs may require diversity for SSCs in this category, or the FSAR may credit them for meeting diversity requirements.

c. lowest safety significance: NSR SSCs 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 Whether a Diversity and Defense in Depth Assessment Is Necessary

A 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."

To accept a failure analysis in lieu of a D3 assessment, the reviewer should determine whether the proposed system is of low safety significance. Section 4 of the attachment to RIS 2002-22, Supplement 1, provides guidance on factors to consider for review of failure analyses of DI&C SSCs.

Acceptance Criteria

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

- The SSC has the characteristics listed in item (c) of Section B.2.1 above, or documented risk insights demonstrate that its level of safety significance is similar to that of SSCs with those characteristics.

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

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

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

3. Diversity and Defense-in-Depth Assessment

A D3 assessment is a systematic approach used to analyze a proposed DI&C system for CCFs that can occur concurrently within a redundant design, for example, within two or more independent divisions. These CCFs could cause the DI&C system to fail to perform its intended safety function or could lead to spurious operations.

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

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

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

- For each event analyzed in the accident analysis sections of the SAR, evaluate whether the D3 assessment indicates that CCF vulnerabilities that might result in loss of function have been adequately addressed.

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

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

General Approach

The reviewer should consider whether the D3 assessment is adequate to identify and defend

against CCF vulnerabilities. Acceptable methods for an applicant to use to address or defend against vulnerabilities include, but are not limited to, the following:

- The applicant eliminated CCF vulnerabilities from further consideration through any of the methods below, either alone or in combination:
  - using diversity within the DI&C system or component (Section B.3.1.1)
  - using testing (Section B.3.1.2)
  - using alternative methods (Section B.3.1.3)
  - for low-safety-significance SSCs, 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 design techniques below:
  - crediting existing systems (Section B.3.2.1)
  - crediting manual operator actions (Section B.3.2.2)
  - crediting a new diverse system (Section B.3.2.3)
- 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 or component (Section B.3.3)

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.[11] As stated in the background section of this BTP, CCFs should be evaluated in a manner consistent with SRM-SECY-93-087. Therefore, the reviewer may apply the methodologies described in this BTP when evaluating spurious operations resulting from CCFs.

Spurious Operation and Integrated Systems[12]

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

When evaluating integrated systems, the reviewer should focus primarily on NSR SSCs that are integrated 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 integrated systems. A secondary focus should be on integration of NSR SSCs that can directly or indirectly affect reactivity (e.g., an NSR rod control system). In some cases, an NSR system may be susceptible to failures not analyzed in the design bases. The reviewer should consider whether a CCF of an integrated NSR DI&C system or platform (e.g., a single platform controlling multiple NSR system functions) could result in spurious operation that would have unacceptable consequences. The reviewer should also consider the level of integration between safety and NSR systems as a potential vulnerability to be addressed in the

---

11 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.

12 The NRC staff is aware that the term "highly integrated" is sometimes used to refer to the special case of safety systems integrated with NSR systems. This BTP does not use that term.

application.[13]

Staff's Evaluation of Spurious Operation

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

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

Many system design and testing attributes, procedures, measures, and practices can significantly reduce the likelihood of a CCF. In a D3 assessment, the following methods can be used to eliminate a potential CCF from further consideration: (1) demonstration of adequate diversity within the DI&C system or component, (2) testing, and (3) other NRC-approved alternative methods within the application. In addition, for SSCs with low 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 such that further evaluation is unnecessary for that portion of the SSC.

The following sections discuss each method.

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

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

The reviewer should determine whether the proposed system contains sufficient diversity to perform the safety function, including diversity within each safety division or among redundant safety divisions of a system. If so, then the potential CCF can be eliminated from further

[13] See IEEE Std 603-1991.

consideration. Section 2.6 of NUREG/CR-6303 identifies six diversity attributes and 25 related diversity criteria that the reviewer can use to determine whether the system includes adequate diversity. Also, NUREG/CR-7007 identifies and develops a baseline set of diversity criteria that may characterize appropriate diversity strategies for mitigating CCF vulnerabilities. However, the quantification methodology described in NUREG/CR-7007 should not be used as the sole basis for justifying adequate diversity.

For example, a proposed digital protection system could implement each credited safety function in two or more independent divisions of the system, each using a different type of digital technology. In this case, the reviewer should determine whether the application includes an analysis reflecting the guidance of NUREG/CR-6303 and NUREG/CR-7007 to demonstrate that the diversity of these independent divisions is sufficient to eliminate a CCF from further consideration.

Acceptance Criteria

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

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

b. Diversity between the different portions of the system or component is sufficient to account for potential spurious operation.

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

d. The diverse portions of the system or component do not have common or shared resources, such as power supplies, memory, bus, or communications modules, whose failure could affect both or all portions. Also, the diverse portions of the system or component do not share engineering or maintenance tools whose failure could affect both or all portions.

e. 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.

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

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

CCF vulnerabilities in DI&C systems or components have two general causes: (1) errors

introduced by the system hardware or software design, and (2) errors or defects introduced during the development and integration of the software, hardware, or software-based logic. When designing an I&C system, the applicant might use a robust (high-quality) development process, in conjunction with thorough system analysis (e.g., failure modes and effects analysis, system theoretic process analysis), to correct many potential design errors in the requirements or specifications for both analog and digital equipment. However, even a high-quality development process cannot completely eliminate latent design defects introduced during the design and integration process.

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

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

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

- every possible combination of inputs, including every possible sequence of inputs (if the system has unused inputs, and the system can force them to a defined safe state (e.g., during a system failure), then those inputs need not meet this criterion)
- for systems with analog inputs, every combination of inputs over the entire operational range of the analog inputs, including defined over-range and under-range conditions
- every possible executable logic path (includes nonsequential logic paths)
- every functional state transition among all modes of operation
- testing results that conform to preestablished test cases to monitor for

correctness of all outputs for every case

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

c. Testing results account for potential spurious operations.

3.1.3 Use of Alternative Methods to Eliminate the Potential for Common-Cause Failure from Further Consideration

Licensees may propose technical approaches to address CCF that this BTP does not describe. These may be alternative methods previously approved by the NRC (e.g., defensive measures), or the licensee may be requesting approval in its application. The NRC's approval of an alternative method should include a supporting technical basis and acceptance criteria for its use. The reviewer should confirm that any previously approved alternative method credited in an application is approved for the use described in the D3 assessment.

If an application credits an alternative method not previously approved by the NRC or not previously approved for the particular application in the D3 assessment, the reviewer should confirm that the application includes a sufficient technical basis for the NRC staff to determine its adequacy. The staff should review such applications on a case-by-case basis.

Acceptance Criteria

If an application uses NRC-approved alternative methods to eliminate a potential CCF from further consideration, the reviewer should conclude that the application provides sufficient information on the credited alternative methods if it includes the following:

a. an identification of the source of vulnerabilities for which the NRC-approved alternative methods are being applied

b. a description of the NRC-approved alternative methods being credited to address the identified vulnerabilities

c. the supporting technical basis and acceptance criteria to demonstrate that these alternative methods are NRC-approved

d. a description of how these alternative methods will address the CCF vulnerability and any potential spurious operations

e. the technical basis explaining why these alternative methods are acceptable for addressing the identified CCF vulnerabilities and preventing or mitigating their effects, including an analysis of how the methods' effectiveness can be demonstrated

As stated above, if the application credits alternative methods not previously approved by the

NRC, the reviewer should determine their adequacy on a case-by-case basis.

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

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

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

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

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

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

Acceptance Criteria

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

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

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

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

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

e. The application documents failure analyses (e.g., FMEAs) that demonstrate how failure effects, including spurious operations, are bounded or taken into account.

3.2 Use of Diverse Means to Mitigate Common-Cause Failures

If a potential CCF vulnerability has not been eliminated from further consideration using the process in Section B.3.1 of this BTP, the reviewer should verify that the application's D3 assessment credits a diverse means to accomplish the same or different function than the safety function disabled by the postulated CCF or to mitigate spurious operations resulting from the postulated CCF. Section 2.6 of NUREG/CR-6303 identifies six diversity attributes and 25 related diversity criteria that the reviewer can use to determine whether the diverse means are adequate to mitigate CCF. In addition, NUREG/CR-7007 identifies and develops a baseline set of diversity criteria that may characterize diversity strategies adequate to address CCF vulnerabilities. However, the quantification methodology described in NUREG/CR-7007 should not be used as the sole basis for justifying adequate diversity.

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

3.2.1 Crediting Existing Systems

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

The reviewer should verify that the applicant considered how the existing system is credited in the facility's licensing basis and described in the existing system's documentation (FSAR, detailed design documents, etc.). Among other things, the reviewer should consider whether

the applicant has appropriately accounted for any unique system design attributes and requirements and potential interconnectivities to other systems. The reviewer should pay particular attention to whether there may be interconnectivities the LAR has not accounted for that may result in the existing system being subject to the same CCF as the proposed DI&C system or component. The reviewer should verify that the application has identified all the features of the existing system that are relevant to demonstrating diversity. In addition, if crediting an existing system could affect the facility's existing licensing basis, then the reviewer should verify that the LAR addresses how the existing system functions would be credited and justified in a revised licensing basis.

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

If prioritization is used, the reviewer should verify that signals to actuate components coming from the new use of the credited existing system and other systems are adequately prioritized to ensure the overall defense-in-depth strategy and existing licensing basis is maintained. The reviewer should also verify that changes to an existing prioritization scheme due to the new use of the credited system are consistent with the existing licensing basis. If there are shared resources (e.g., priority modules), the reviewer should consider whether the credited existing system has priority over the resources in regard to its safety and protection functions, such that these functions are always carried out first. DI&C-ISG-04 provides guidance on prioritization of control and protection systems sharing components. Note: In some cases, certain components may have more than one safe state; the reviewer should consider whether all safe states were described in the priority scheme.

Acceptance Criteria

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

a. If NSR equipment is used in the diverse system, the equipment is of sufficient quality to

perform the necessary function(s) during the associated event conditions. Sufficient quality can be achieved, for example, through application of the alternative treatment requirements developed for implementation of 10 CFR 50.69 or the ATWS quality assurance guidance set forth in GL 85-06.

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

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

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

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

3.2.2 Crediting Manual Operator Action

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

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

If the applicant proposed the use of equipment outside the MCR to perform the credited manual operator action, the reviewer should consider whether this equipment is vulnerable to the same CCF as the safety system and whether the applicant demonstrated that the equipment will be

reliable, available, and accessible under the postulated event conditions. The reviewer may use the HFE principles and criteria identified in SRP Chapter 18 to evaluate the applicant's selection and design of the displays and controls. In addition, the reviewer may use the guidance in NUREG-1764, Revision 1, to perform a risk-informed evaluation of the application.

Protective Actions Initiated Solely by Manual Actions

Protective actions initiated solely by manual controls must be verified to meet appropriate HFE criteria and to use adequate equipment and controls. RG 1.62 provides guidance for evaluating the adequacy of equipment and controls used to manually initiate protective actions otherwise provided by automatically initiated safety systems. SRP Chapter 18, Attachment A, provides guidance for evaluating credited manual actions.

Acceptance Criteria

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, Attachment A. The application describes human performance requirements and relates them to the plant safety criteria. The application employs recognized human factors standards and design techniques to support the described human performance requirements.

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

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

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

3.2.3 Crediting a New Diverse System

The applicant may propose a new diverse system (e.g., a diverse actuation system) as a diverse means of accomplishing the same or a different function credited in the D3 assessment or of mitigating spurious operation due to CCF. In this case, the reviewer should determine whether the application demonstrates that (1) the functions performed by this diverse means suffice to maintain plant conditions within specified acceptance criteria for the associated DBE, and (2) sufficient diversity exists between the new system and the proposed DI&C system so

that they are not vulnerable to the same postulated CCF. The reviewer should determine whether the diverse means credited and the digital design of the proposed system are vulnerable to the same CCF. Section 2.6 of NUREG/CR-6303 identifies six diversity attributes and 25 related diversity criteria that the reviewer can use to determine whether the new diverse system is adequate to mitigate the CCF.

The new diverse system may be an NSR system if it is of sufficient quality to perform the necessary functions under the associated event conditions. The reviewer should consider whether the new diverse system can function under the event conditions expected and whether it is of adequate quality, which can be verified, for example, based on the alternative treatment requirements developed for implementation of 10 CFR 50.69, or on the ATWS quality assurance guidance in GL 85-06.

Prioritization

If a new diverse system is implemented, the reviewer should verify that the signals to actuate components coming from the different systems are appropriately prioritized to maintain the overall defense-in-depth strategy. If the proposed DI&C system and the new diverse system share resources (e.g., priority modules), the reviewer should consider whether the proposed DI&C system has priority in the use of shared resources in regard to its safety and protection functions, so that safety and protection functions are always carried out first. DI&C-ISG-04 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

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

a. If NSR equipment is used in the diverse system, the equipment is of sufficient quality to perform the necessary function(s) during the associated event conditions. Sufficient quality can be achieved, for example, through application of the alternative treatment requirements developed for implementation of 10 CFR 50.69 or the ATWS quality assurance guidance set forth in GL 85-06.

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

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

d. Common resources shared by proposed system(s), other systems, and manual operator actions are controlled by prioritization of commands consistent with the guidance in DI&C-ISG-04. The basis for the prioritization should be documented.

3.3 Consequences of a Common-Cause Failure May Be Acceptable

If the applicant has not been eliminated from further consideration using the process in Section B.3.1 of this BTP and has not credited a diverse means to accomplish the vulnerabilities using the methods in Section B.3.2, then the reviewer should verify the application demonstrates that consequences of residual identified CCF remain acceptable. In this case, the reviewer should consider the applicant's analysis demonstrates that, should the CCF occur, the facility will remain within the acceptance criteria defined in the FSAR or the LAR for the limiting events applicable to the proposed DI&C system or component.

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

Acceptance Criteria

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

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

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

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

Point 4 of the NRC's position on D3 states that the applicant shall provide a set of displays and controls in the MCR for manual system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. Section B.1.2 defines critical safety functions. RG 1.62 outlines important design criteria for I&C equipment used by plant operators for manual initiation of protective actions.

The reviewer should consider whether displays and manual controls provided to meet point 4 are not vulnerable to the same CCF as the proposed DI&C system. For example, the point at which the credited manual controls are connected to the safety equipment should be downstream of the equipment that can be adversely affected by a CCF. The reviewer should confirm that the applicant does not credit the same digital platform or analog technology for point 3 (e.g., to mitigate DBEs). Point 4 specifies that the MCR displays and controls shall be independent and diverse from the digital platform or analog technology identified for points 1 and 3.

If they are not vulnerable to the same CCF, the applicant may credit some or all of the displays and manual controls provided to meet point 4 as the diverse means called for under point 3, as described in Section B.3.2.2 of this BTP. In most cases, when displays and manual controls are credited as the diverse means for point 3, they may also be credited for point 4. However, if the diverse means credited for point 3 are not located in the MCR, then they are not sufficient to meet point 4.

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

Acceptance Criteria

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

a. The proposed manual actions credited to accomplish safety functions that would otherwise have been accomplished by automatic safety systems are both feasible and reliable, as demonstrated through an HFE analysis and assessment process, such as the one described in SRP Chapter 18. Section B.3.2.2 of this BTP presents the acceptance criteria for manual actions.

b. The application identifies the minimum inventory of displays and controls in the MCR, and this minimum inventory allows the operator to effectively monitor and control the critical safety parameters of reactivity, core heat removal, and reactor coolant inventory. The minimum inventory also allows the operator to initiate and monitor the status of containment isolation and containment integrity.

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

d. The manual controls for critical safety functions are at the system or division level and are located within the MCR. For plants licensed to allow one division to be continuously out of service, the diverse manual actuation applies to at least one division that is in

service.

e. If NSR equipment is used, its quality and reliability are adequate to support the manual operator action during the associated event conditions. Equipment quality can be verified, for example, based on the alternative treatment requirements developed for implementation of 10 CFR 50.69, or on the ATWS quality assurance guidance in GL 85-06.

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

5. Information for Interdisciplinary NRC Staff Review

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

a. the applicant's documentation of its safety-significance determination for a proposed DI&C system and the supporting technical basis. If risk insights from plant-specific PRAs are used to inform such a determination, the PRA results should be reviewed by the staff.

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

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

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

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

c. for systems that the applicant has not assessed for CCF, information showing that all conditions introduced by the proposed modification are bounded by the acceptance

criteria defined in the FSAR or the LAR for the limiting events applicable to the proposed DI&C system or component

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

- controls and displays provided in the MCR to perform manual system- or division-level actuation of critical safety functions
- 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
- controls and displays have sufficient quality to support the manual operator actions during the associated event conditions, if the equipment used is NSR

6. Additional Items for Consideration

The reviewer should use the acceptance criteria described in Section B.3 of this BTP and the detailed guidance of NUREG/CR-6303 and NUREG/CR-7007 to evaluate the applicant's D3 assessment. During this evaluation, the reviewer should consider the topics described below.

6.1 System Representation as Blocks

As described in NUREG/CR-6303, a block is a representation of a physical subset of equipment and software for which it can be credibly assumed that internal failures, including the effects of latent design defects, will not propagate to equipment or software outside of the block. A block can also be a software macro or subroutine, such as a voting block or a proportional–integral–derivative block, that is used by multiple functional applications. Representations of systems or components using blocks may not show the inner workings of each block.

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

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

6.2 Documentation of Assumptions

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

6.3 Identification of Alternate Trip or Initiation Sequences

The reviewer should verify that the applicant's assessment includes thermal-hydraulic analyses of the sequence of events that would occur if the primary trip channel failed to trip the reactor or actuate ESFs. The thermal-hydraulic 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.

6.4 Identification of Alternative Mitigation Capability

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

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

6.5 Justification for Not Correcting Specific Vulnerabilities

The reviewer should consider whether the applicant provided justification for not correcting any identified vulnerabilities that the application leaves unresolved. Such justification might include, for example, design attributes (e.g., redundancy, diversity, independence) and diverse actuation or mitigation capabilities, as well as previously NRC-approved credited manual operator actions in the licensing basis to address AOOs or PAs. The 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. Code of Federal Regulations* (CFR), “Domestic Licensing of Production and Utilization Facilities,” Part 50, Chapter I, Title 10, “Energy.”

2. CFR, “Licenses, Certifications, and Approvals for Nuclear Power Plants,” Part 52, Chapter I, Title 10, “Energy.”

3. CFR, “Reactor site criteria,” Part 100, Chapter I, Title 10, “Energy.”

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

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

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

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

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

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

10. U.S. Nuclear Regulatory Commission, “Manual Initiation of Protective Actions,” Regulatory Guide 1.62, Revision 1, June 2010.

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

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

13. U.S. Nuclear Regulatory Commission, “Criteria for Use of Computers in Safety Systems of Nuclear Power Plants,” Regulatory Guide 1.152.

14. U.S. Nuclear Regulatory Commission, “Cyber Security Programs for Nuclear Facilities,” Regulatory Guide 5.71.

15. U.S. Nuclear Regulatory Commission, “Regulatory Requirements, Acceptance Criteria, and Guidelines for Instrumentation and Control Systems Important to Safety,” NUREG-0800, Section 7.1-T.

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

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

18. U.S. Nuclear Regulatory Commission, “Cyber Security Plan,” NUREG-0800, Section 13.6.6.

19. U.S. Nuclear Regulatory Commission, “Transient and Accident Analysis,” NUREG-0800, Chapter 15.

20. U.S. Nuclear Regulatory Commission, “Human Factors Engineering,” NUREG-0800, Chapter 18, Revision 3, December 2016.

21. U.S. Nuclear Regulatory Commission, “Review Process for Digital Instrumentation and Control Systems,” NUREG-0800, Appendix 7.0-A.

22. U.S. Nuclear Regulatory Commission, “Guidance on Self-Test and Surveillance Test Provisions,” NUREG-0800, BTP 7-17.

23. U.S. Nuclear Regulatory Commission, “Guidance on Digital Computer Real-Time Performance,” NUREG-0800, BTP 7-21.

24. U.S. Nuclear Regulatory Commission, “Guidance for the Review of Changes to Human Actions,” NUREG-1764, Revision 1, September 2007.

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

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

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

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

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

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

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

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

Paperwork Reduction Act Statement

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

Public Protection Notification

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

BTP Section 7-19

Description of Changes

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

This branch technical position section updates the guidance previously provided in Revision 7, issued August 2016 (Agencywide Documents Access and Management System Accession No. ML16019A344).

The main purpose of this update is to clarify sections of the guidance that proved challenging to implement, according to feedback received by internal and external stakeholders. The update improves readability and flow to make it clear to the reader that there is an established process for analyzing potential vulnerabilities to common-cause failures resulting from latent design defects in digital technology, in particular within hardware, and software or software-based logic. The update clarifies the scope of applicability for all users and clearly states that this guidance does not apply to the change process in Title 10 of the *Code of Federal Regulations* 50.59, "Changes, tests and experiments." The update provides for structures, systems, and components of differing safety significance, so that an adequate demonstration of safety is consistently applied. It also clarifies specific areas of guidance, such as diversity and testing, and adds the concepts of alternative methods, qualitative assessment, and supporting failure analysis as means of addressing common-cause failures.