NUREG-0800

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 – October 2020

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). References to industry standards incorporated by reference into regulations (Institute of Electrical and Electronics Engineers (IEEE) Standard (Std) 279-1968, IEEE Std 279-1971, and IEEE Std 603-1991) and industry standards that are not endorsed by the agency do include the associated year in this BTP. See Table 7-1 to ensure that the appropriate RGs and endorsed industry standards are used for the review.

A. BACKGROUND

Digital technology offers significant operational and maintenance benefits for instrumentation and control (I&C) systems of nuclear power plants (NPPs). Digital I&C (DI&C) systems are composed 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, software includes 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 application of 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 result in two different effects: (1) a loss of the capability to perform a safety function or initiate a plant transient, or (2) initiate the operation of a function without a valid demand or result in erroneous (i.e., spurious) system actions. 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 Staff Requirements Memorandum (SRM) on SECY 93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light Water Reactor (ALWR) Designs," dated July 21, 1993, the NRC considers CCF in DI&C

[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 under 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.

systems to be a beyond-design-basis event (BDBE). 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 the identification and evaluation of potential consequences of a postulated CCF more challenging.

Generally, DI&C systems containing software or logic cannot be fully tested except for a limited number of very simple SSC designs, nor can their failure modes be completely predicted because software includes too many potential failure modes to deterministically predict. 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 DI&C systems, or (2) when DI&C systems are integrated and interconnected (e.g., shared resources).

CCF vulnerabilities of DI&C systems or components are addressed based on the principles of defense-in-depth. Under these principles, the operation of facility systems is modeled as a series of successive layers of defense (referred to as “echelons of defense”), each of which would need to be defeated for the consequences of a failure due to CCF to cause 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, type and use of shared resources. NUREG/CR-6303, “Method for Performing Diversity and Defense in Depth Analyses of Reactor Protection Systems,” issued December 1994, describes defense in depth for NPPs. For example, Section 2.2 of NUREG/CR-6303 identifies the normal reactor control systems, the reactor trip system, the ESF actuation system, 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 result in adverse plant consequences. Staff guidance for evaluating real-time deterministic processing is presented in SRP sections 7.0-A and BTP 7-21. Staff guidance for evaluating control of access is presented in Table 2 Item B.3.1, and Table 3 Item C.7 of SRP Chapter 13.6.6. BTP 7-17 provides staff guidance for the evaluation of self-test features.

Over the years, the NRC staff has approved applications with various design solutions to

address CCF vulnerabilities in DI&C systems. In some cases, multiple design solutions have been applied within different parts of a single DI&C system. During the review of these applications, the NRC staff has evaluated several different solutions that successfully address CCF vulnerabilities. Based on that experience, the staff recognizes that one standard solution may not be applicable for all DI&C systems.

1. Regulatory Basis

The regulations listed below may not necessarily apply to all applicants. The applicability of the regulatory requirements is determined by the plant-specific licensing basis and any proposed changes to the licensing basis associated with the proposed 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 that protection systems be consistent with the plant-specific licensing basis or may comply with IEEE Std 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," and the IEEE Std 603-1991 correction sheet dated January 30, 1995.

- For NPPs with CPs issued between January 1, 1971, and May 13, 1999, 10 CFR 50.55a(h) requires that protection systems comply with the requirements stated in 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.

- 10 CFR Part 50, "Domestic licensing of production and utilization facilities," Appendix A, "General Design Criteria for Nuclear Power Plants," General Design Criterion (GDC) 22, "Protection System Independence," states,

  > 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.

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

- 10 CFR Part 50, “Domestic licensing of production and utilization facilities,” Appendix A, GDC 25, “Protection system requirements for reactivity control malfunctions” states that 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.

- 10 CFR Part 50, “Domestic licensing of production and utilization facilities,” Appendix A, GDC 26, “Reactivity control system redundancy and capability.”

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

- 10 CFR Part 100, “Reactor site criteria,” Subpart A, applies to holders of and applicants for operating licenses whose construction permits were issued before January 10, 1997, and required the construction permit 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 digital I&C design by considering the consequences of a CCF concurrent with a DBE.

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

- 10 CFR 50.69, “Risk-informed categorization and treatment of structures, systems and components for nuclear power reactors,” allows 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 structures, systems, and components of its nuclear power reactor.

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

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

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

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

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

2. Relevant Guidance

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

- NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems," summarizes several defense-in-depth and diversity (D3) analyses performed after 1990 and presents a method for performing analyses of proposed DI&C systems to identify design vulnerabilities to common mode failures[4] and to ensure there is adequate defense in depth to address them, including the use of additional diversity within the design. NUREG/CR-6303 presents an analysis method that postulates common-mode failures that could occur within digital reactor protection systems and determines what portions of a design need to include additional D3 measures to address such failures.

- NUREG/CR-7007, "Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems," issued December 2008, provides guidance and strategies for including diversity for mitigating potential vulnerabilities that can lead to a CCF in a given safety-related system based on a D3 assessment of the system that shows a need for such diversity. NUREG/CR-7007 identifies and develops a baseline set of diversity criteria that may constitute appropriate mitigating diversity strategies to address 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, Item II.Q, as clarified by SRM-SECY-93-087, Item 18, describes the NRC position concerning defense against potential common mode failures in digital I&C systems.

- SECY-18-0090 provides 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 with respect to 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.

[4] It should be noted 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.

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

- NUREG-0800, SRP Table 7-1, “Regulatory Requirements, Acceptance Criteria, and Guidelines for Instrumentation and Control Systems Important to Safety.”

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

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

- NUREG-0800, SRP Chapter 18, “Human Factors Engineering,” defines a methodology, applicable to both existing and new reactors, for evaluating manual operator action as a diverse means of coping with AOOs and PAs that are concurrent with a CCF due to latent design defects that disable a safety function credited in the SAR. SRP Chapter 18, 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 nuclear power plants, and (2) in applications for CPs, OLs, COLs, DCs, SDAs, and MLs. This BTP is not applicable to proposed modifications performed under the change process in 10 CFR 50.59, “Changes, tests and experiments.”

Review criteria for single random failures and cascading failures from shared resources (i.e., not due to latent design defects in digital I&C SSCs) are not covered in this BTP. The reviewer can find guidance for addressing single failures in systems credited to perform safety functions in Regulatory Guide 1.53, “Application of the Single Failure Criterion to Safety Systems.” Also, SRP Section 7.7, “Control Systems,” provides guidance for the analysis of postulated failures in NSR systems.

4. Purpose

This BTP provides the U.S. Nuclear Regulatory Commission (NRC) staff with guidance for evaluating an applicant's assessment of the adequacy of defense in depth and diversity (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 CCF outcomes on plant safety.

This BTP also provides guidance for the staff to review:

- the appropriateness of the methods selected by an applicant to perform a D3 assessment, including any categorization of proposed DI&C SSCs based on the safety significance of the functions performed by the proposed DI&C SSCs.

- 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 the potential for CCF from further consideration[5].

- an applicant's use of diverse external equipment, including manual controls and displays to mitigate a potential CCF, and other measures to ensure conformance with the NRC's position on addressing potential 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. This BTP 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 staff evaluation of the acceptability of the applicant's D3 assessment of proposed DI&C systems.[6]

For this evaluation, the reviewer should confirm the following is included in the application:

- 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;

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

[6] The review acceptance criteria in this BTP are structured as guidance to the NRC staff so that the NRC 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.

- A documented basis for any safety significance determinations used in the application;
- A failure analysis for any SSCs excluded from a D3 assessment; and
- A description of any D3 assessment including:
  - 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 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, mitigate, or withstand or cope with (i.e., accept the consequences of) such possible CCFs and sources of CCF vulnerability that can result in spurious operations.

1.1. Four Common-Cause Failure Positions and Discussion

The foundation of BTP 7-19 is the "NRC position on D3" from Staff Requirements Memorandum (SRM)-SECY 93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light Water Reactor (ALWR) Designs," dated July 21, 1993. The four positions stated in SRM-SECY-93-087 are quoted below:

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

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

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

Position 4: A set of displays and controls located in the main control room shall be provided for

manual, system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. The displays and controls shall be independent and diverse from the safety computer system identified in [Positions] 1 and 3 above.[7]

The guiding principles in SECY-18-0090 clarify that the D3 assessment described in Position 1 should be commensurate with the safety significance of the proposed DI&C system or component. Section B.2 provides guidance to review an applicant's safety significance determinations, if any are used, and Section B.3.1 provides guidance for reviewing an applicant's use of those determinations in the D3 assessment. Section B.2 also provides guidance on reviewing an applicant's determination that a D3 assessment is not necessary based on a failure analysis.

Position 2 uses the term "best estimate methods," but this term is somewhat out of date; the same 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, and also includes acceptance criteria that are less conservative than the acceptance criteria defined in the Final Safety Analysis Report, as updated (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

The guiding principles in SECY-18-0090 clarify that, in addition to methods using realistic assumptions identified in Position 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 a postulated CCF could disable a safety function, then Position 3 directs that a diverse means be provided to perform the 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 be comprised of equipment that is NSR with a documented basis that the diverse means is of sufficient quality and is not subject to the same CCF vulnerability. Examples of methods for demonstrating sufficient quality include application

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

of the alternative treatment provided in 10 CFR 50.69(d)[8] or quality controls or measures developed in accordance with GL 85-06, which provides quality assurance guidance for ATWS. SECY-18-0090 clarifies that use of either automatic or manual actuation within an acceptable time frame is an acceptable means of diverse actuation. If the D3 assessment demonstrates that a possible CCF can be reasonably mitigated through other means (such as through the use of 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 subject to the same source of CCF vulnerability that could disable the safety function.

If a diverse means is part of a safety-related system, it would then be subject to 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 IEEE Std 603-1991, Clause 5.6.3 requirements for separation and independence between safety-related systems and NSR systems apply.

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

Further, if not subject to the same CCF vulnerability as the proposed safety-related DI&C system, some of these displays and manual controls from Position 4 may be credited as all or part of the diverse means provided to address Position 3. The Position 4 phrase "safety computer system identified in [Positions] 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 Position 4:

- reactivity control
- core heat removal
- reactor coolant inventory

[8] While required for implementing § 50.69, the quality assurance measures called for by § 50.69(d) are not required for the equipment comprising the diverse means but can serve as guidance for the quality of that equipment.
[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 provide any clarification for Position 4.

- containment isolation
- containment integrity

Other safety functions an applicant identifies in the SAR may not always be “critical safety functions,” as used in SRM-SECY-93-087. NUREG-0737, Supplement No. 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 to implement Principle 3 in SECY-18-90, 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 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 purposes of this BTP, a safety-significant function is one whose degradation or loss could result in a significant adverse effect on defense-in-depth, safety margin, or risk. For example, due to the immediacy of the responses 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 final SAR.

An assessment to address CCF for an RTS should be more rigorous than an assessment for a safety-related Main Control Room Heating, Venting, and Air Conditioning (HVAC) chiller. While the HVAC chiller is a safety-related system that maintains certain temperature and humidity in the MCR for equipment and personnel to operate properly, a failure of this system is not as significant as the failure of the RTS because operators will have operating procedures or diverse means to control MCR temperature and humidity and will shut down the plant, 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 and determine the safety significance of the DI&C system. The reviewer should confirm that the application documents the basis for determining the safety significance of the proposed system, 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 SSC should be assessed in accordance with the appropriate methods for the highest safety significant SSC that is integrated or interconnected. Staff reviewers should consider whether the applicant included a clear description of the proposed DI&C system or component to identify (1) shared resources, (2) interconnection with other systems, and (2) whether the modification has the potential to reduce the redundancy, diversity, separation, or independence of systems described in the facility's safety analysis report (SAR).

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 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 ESF logic and also includes 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 has been categorized in the highest safety significant SSC category. In this example, the reviewer should determine whether the D3 assessment for these interconnected or integrated systems conforms to the criteria in Sections B.3.1 through B.3.3 for a D3 assessment for those 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 following acceptance criteria. The use of risk insights, such as from a site-specific PRA, to demonstrate that an SSC is less safety-significant than these characteristics would indicate should be reviewed on a case-by-case basis.

a. High Safety Significance: Safety-related SSCs that Perform Safety-Significant Functions

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

   - Are credited in the FSAR to perform design functions that are significant contributors to plant safety.

   - Are relied upon to initiate and complete control actions essential to maintain plant parameters within acceptable limits established for a DBE, or to maintain the plant in a safe state after it has reached safe shutdown.

   - Failure could directly lead to accident conditions that may cause unacceptable consequences (e.g., exceeds siting dose guidelines for a DBE) if no other automatic systems are available to provide the safety function, or no pre-planned manual operator actions have been validated to provide the safety function.

- Functional diversity, to the extent practical, is required by GDC 22.

b. Lower Safety Significance: Safety-Related SSCs that do not Perform Safety-Significant Functions and Non-safety-related SSCs that do Perform Safety-Significant Functions

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

- Provides an auxiliary or indirect function in the achievement or maintenance of a safety-related function.
- Performs an NSR design function that is a significant contributor to plant safety.
- Capable of directly changing the reactivity or power level of the reactor and whose failure could initiate an accident sequence or could adversely affect the integrity of a safety barrier (i.e., fuel cladding, reactor vessel, and 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: Non-safety-related SSCs that Do Not Perform Safety-Significant Functions

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

- Perform functions that are not considered significant contributors to plant safety.
- Do not have a direct effect on reactivity or power level of the reactor or affect the integrity of a safety barrier (i.e., fuel cladding, reactor vessel, and containment).

2.2 Using Safety Significance to Determine whether a D3 Assessment is Necessary

A D3 assessment is necessary for all systems determined to be of higher safety significance. As stated in SECY-18-90, a D3 assessment is used to demonstrate "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 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." The reviewer should determine whether the proposed system is of low safety significance to accept the failure analysis in lieu of a D3 assessment.

Section 4, "Failure Analysis," of the attachment to RIS 2002-22, Supplement 1, provides guidance on factors that are important to consider for review of failure analyses of digital I&C SSC.

Acceptance Criteria

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

- The SSC has the characteristics described in paragraph c. of section B.2.1 above or documented risk insights demonstrate that the SSC has a similar level of safety significance as 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. Defense-in-Depth and Diversity Assessment

A D3 assessment is a systematic approach an applicant uses to analyze the proposed design of a DI&C system for CCFs that can occur concurrently within a redundant design, such as within two or more independent divisions. These CCFs could lead to a failure of the DI&C system to perform its intended safety function or result in spurious operation.

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

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

- Confirm that a D3 assessment was performed for a proposed system or component to determine whether vulnerabilities to a CCF have been adequately addressed.
- For each event analyzed in the accident analysis sections of the SAR, assess whether the results of the D3 assessment indicates that vulnerabilities to CCF that might result in loss of function have been adequately addressed.

- Evaluate whether the results of the D3 assessment indicates that vulnerabilities to CCF that might result in spurious operation have been adequately addressed.

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

General Approach

The reviewer should consider the adequacy of the D3 assessment to identify and provide defense against CCF vulnerabilities. Acceptable methods an applicant may use to address or defend against vulnerabilities include, but are not limited to the following:

- The applicant eliminated CCF vulnerabilities from further consideration using any of the methods described below, either alone or in combination:
  - Using diversity within the digital instrumentation and control 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 or mitigated consequences from CCF vulnerabilities using design techniques described below:
  - Crediting existing systems. (Section B.3.2.1).
  - Crediting manual operator action. (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, so no defense against CCF vulnerabilities is provided. (Section B.3.3).

If the applicant uses multiple strategies to address or defend against CCF vulnerabilities in different portions of a system, then the reviewer should evaluate how the applicant analyzed the potential for addressing CCF vulnerabilities and how each method was applied. For example, for one portion of the system, the applicant might eliminate the CCF from further consideration, while the other portions of the system rely on diverse I&C systems to mitigate the CCF vulnerability.

Spurious Operation as a Result of CCF

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

result in an event that has 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, there may be circumstances in which a spurious operation would not occur until a particular signal or set of signals are present. In these cases, the spurious operation would not occur immediately upon system startup, but rather could occur under certain plant conditions. This spurious operation is still self-announcing (by the actuated system), even if failure did not occur on initial test or startup.

Due to the potential consequences of a spurious operation, a failure of a system to actuate might not be the most limiting failure. This is true especially when analyzing the time needed for identifying and responding to conditions resulting from spurious operation in DI&C systems. In some cases, a failure to trip might not be as limiting as a partial actuation. For example, a partial actuation of an emergency core cooling system (i.e., spurious operation of a single division) with false indication of a successful actuation may take an operator longer to evaluate and correct than a total failure to send any actuation signal. Therefore, the reviewer should consider both the possibility of 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 "beyond design basis" events and are within the scope of this BTP.[11] As stated in the Background section of this BTP, CCF should be evaluated in a manner consistent with SRM-SECY 93-087. Therefore, the reviewer may consider the methodologies described in this BTP when evaluating spurious operations resulting from CCFs in a proposed system.

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 the identification of CCF vulnerabilities and evaluation of potential consequences of a postulated CCF challenging. System integration and interconnectivities including shared resources have the potential to reduce overall defense-in-depth (e.g., reduction in independence) for a plant.

With respect to integrated systems, the primary focus should be on NSR SSCs that are integrated with safety-related SSCs. This is the primary focus because there are particular regulatory requirements for safety-related SSCs that separately address CCF vulnerabilities in

[11] Spurious operations addressed "within the design basis" include spurious operations that occur as a result of single failures (including cascading effects) or single malfunctions. Consistent with regulatory requirements such as those of GDC 25 or incorporated by reference in 10 CFR 50.55a(h) (IEEE Std 279-1971 or IEEE Std 603-1991), spurious operations as a result of single failures and single malfunctions are expected during with 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 a special cases of safety systems integrated with NSR systems. This BTP does not use the that term.

integrated systems (e.g., independence and quality requirements). 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., multiple NSR system functions controlled by the same platform) has the potential to 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 application.[13]

Staff's Evaluation of Spurious Operation

The reviewer should consider whether spurious operation resulting from CCF is addressed as part of the D3 assessment along with loss of function resulting from CCF. One important distinction is that unlike CCF resulting in a failure to perform a function, spurious operation is considered an initiating event only, i.e., 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 contribute to significantly reducing the likelihood of a CCF. For the purposes of the D3 assessment, some methods can be used to eliminate a potential CCF from further consideration. These methods include: (1) demonstration of adequate diversity within the DI&C system or component, (2) testing, and (3) other NRC-approved alternative methods within the design. In addition, for SSCs with low safety significance, a qualitative assessment and failure analysis that shows the likelihood of failure is sufficiently low can be used to eliminate CCF from further consideration. The reviewer should determine whether the application demonstrates that the use of these methods, in any combination or on their own, meets the criteria in this BTP to eliminate the potential CCF from further consideration.

Even if these methods do not eliminate all aspects of the CCF vulnerability from further consideration, the reviewer should consider whether the applicant has sufficiently minimized the likelihood of a CCF occurring in any particular portion of the SSC such that the applicant does not need to perform further evaluation for that portion of the system or component. 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 the I&C system or component constitutes using a different technique, schemes, features, or additions to eliminate a CCF from further consideration. If diversity is used, each diverse portion of the system or component has different potential latent design defects, such that a failure in one portion will not necessarily imply a failure in the other portion. Diversity can be implemented by different techniques, such as different technologies, algorithms or logics,

[13] See IEEE Std 603-1991.

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 vulnerability.

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

For example, a digital protection system could be designed such that each credited safety function is implemented in two (or more) independent divisions of the protection system that use different types of digital technology. In this case, the reviewer should determine whether the application includes an analysis comparable to the guidance of NUREG/CR-6303 and NUREG/CR-7007 to demonstrate that the diversity attributes between these different divisions of the digital protection system are adequate to eliminate a CCF such that further consideration is unnecessary.

Acceptance Criteria

If the acceptance criteria identified below are met, the reviewer should reach a conclusion 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:

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

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

c. Diversity is adequate between the diverse portions of the system or component to perform the safety function without reliance on the performance of common components, and the SSCs and software of each diverse portion is not subject to the same sources of CCF.

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 that could affect both portions. Also, the diverse portions of the system or component do not share engineering or maintenance tools that could affect both portions.

e. Each diverse portion used to perform the credited safety functions is shown to be

reliable and available for the plant conditions during which the associated event is expected to be prevented or mitigated.

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

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

When considering CCF vulnerabilities in DI&C systems or components, there are two general areas of concern: (1) CCF resulting from errors introduced by the system hardware or software design, and (2) CCF resulting from errors or defects introduced during the development and integration of the software, hardware, or software-based logic. During the design of 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 address many potential design errors in the system or component requirements or specifications for both analog and digital equipment. However, even a high-quality development process cannot completely eliminate all potential latent design defects introduced during the design and integration process of the DI&C system.

Thorough testing can help to identify latent design defects in the design of DI&C systems, provided a design is simple enough to enable 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, tested, and corrected such that the DI&C system and 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 such cases, the reviewer should consider whether the technical basis for these testing methods is acceptable.

Acceptance Criteria

If the acceptance criteria identified below are met, the reviewer should reach a conclusion that the application provides adequate information on the test results and testing methodology for a device or component such that a potential CCF can be eliminated from further consideration. The acceptance criteria are:

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

    - 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 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 to guarantee that the system will perform the same functions as those specified and 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 are not described in this BTP. These "alternative methods" (e.g. defensive measures) may be previously approved by the NRC or the licensee may be requesting approval in its application. The NRC approval should include a supporting technical basis and acceptance criteria for use of the alternative method specified by the applicant. The reviewer should confirm that any previously-approved alternative method credited in an application is approved for the use described in the D3 assessment.

For an application that credits alternative methods not previously approved by the NRC or not previously approved for the alternative method's particular application in the D3 assessment, the reviewer should confirm that the application includes an adequate technical basis for the NRC staff to determine the adequacy of the alternative method. Such applications should be reviewed on a case-by-case basis.

Acceptance Criteria

If the application credits the use of NRC-approved alternative methods to eliminate the potential for a CCF from further consideration, the reviewer should reach a conclusion that the application provides sufficient information on the credited alternative method to eliminate a potential CCF from further consideration if the application 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. includes the supporting technical basis and acceptance criteria to demonstrate that these alternative methods are NRC-approved.

d. a description of how the CCF vulnerability, including any potential for spurious operations, will be prevented by the proposed alternative method;

e. the technical basis that describes why the selected alternative methods are acceptable to address the identified vulnerabilities such that the effects of a CCF will be prevented, including an analysis of how the effectiveness of the methods credited can be demonstrated.

If the application credits the use of alternative methods to eliminate the potential for a CCF from further consideration that the NRC has not previously approved, the reviewer should determine the adequacy of the alternative methods 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 to assess the likelihood of failure due to CCF in DI&C systems and components. This methodology is called a “qualitative assessment.” RIS 2002-22, Supplement 1, identifies the 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, which is referred to as “sufficiently low.” The “sufficiently low” definition compares likelihood of failure of a proposed DI&C system or component to other failures documented in FSAR.

The qualitative assessment is a less technically rigorous method of a 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 to demonstrate that a system will exhibit a low likelihood of failure (i.e. low likelihood of CCF occurring). The technical basis includes: (1) three factors used to demonstrate 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 whether 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. These are the factors to consider for a qualitative assessment:

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

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

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

Second, the reviewer should consider any failure analysis included in the qualitative assessment. This analysis includes information from engineering design work, such as FMEAs and FTAs. The reviewer should consider whether this failure analysis supports the factors above by, for example, demonstrating that identified vulnerabilities to CCF exhibit a low likelihood of occurrence.

Acceptance Criteria

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

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

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

c. The applicable operating experience on the DI&C system or component collectively supports a conclusion that the DI&C system will operate with high reliability for the intended application. Operating experience in some cases can serve to compensate for weakness in addressing criteria (a) and (b).

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

e. Failure analyses (e.g., FMEAs) that demonstrate how failure effects, including spurious operations, are bounded or accounted for, are documented.

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 a D3 assessment in the application 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 NRC reviewers can use to consider 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 constitute mitigating diversity strategies adequate to address

vulnerabilities to CCFs. 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 acceptable to address Position 3. These diverse means include existing system, manual operator action, or new diverse systems.

3.2.1. Crediting Existing Systems

An existing reliable I&C system can be used as a diverse means to provide the same or a different function credited in the D3 assessment or to mitigate spurious operation resulting from CCF. The analysis in the LAR of the function performed by this existing I&C system should demonstrate that the result of the CCF meets the acceptance criteria defined in the FSAR or the LAR for the limiting events applicable to the proposed DI&C system or component. If an existing system is credited, then the reviewer should verify that the applicant performed an analysis to demonstrate that the credited and the proposed system are not subject to the same postulated CCF.

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

<u>Acceptance Criteria</u>

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

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

b. The credited equipment is not subject to the same postulated CCF or sources of

CCF as the proposed DI&C system.

c. The credited equipment (1) has the capability of sensing and responding to the same plant conditions as the affected system if performing the same safety function, or (2) is capable of sensing and responding to alternative plant conditions if performing a different function, including mitigating spurious operation. For both options, the capabilities for sensing and responding ensure that plant conditions stay within the acceptance criteria specified for each AOO or PA in the SAR.

3.2.2. Crediting Manual Operator Action

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

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) 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 application should include information to demonstrate that the equipment is of adequate quality, which can be achieved, for example, through application of the alternative treatment requirements provided in 10 CFR 50.69 or the ATWS quality assurance guidance set forth in GL 85-06.

If the applicant proposed using equipment outside of the MCR to perform the credited manual operator action, the reviewer should consider whether this equipment is subject to the same CCF vulnerability as the safety system used. Also, the reviewer should consider whether the reliability, availability, and accessibility of the equipment under the postulated event conditions has be demonstrated. 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.

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

Protective actions initiated solely by manual controls are subject to the consideration of appropriate HFE criteria and the use of adequate equipment and controls. RG 1.62 provides guidance for evaluating the adequacy of equipment and controls used as a means for manual initiation of protective actions otherwise provided by automatically initiated safety systems, or as

a method diverse from automatic initiation. SRP Chapter 18, Attachment A, provides guidance for evaluating the adequacy of human factors engineering the applicant performed to validate the feasibility and reliability of the proposed manual actions.

Acceptance Criteria

If the acceptance criteria identified below are met, the reviewer should reach a conclusion that using the proposed manual operator action is acceptable. The acceptance criteria are:

a. The proposed manual operator actions have been validated using an HFE process, such as that specified in SRP Chapter 18, Attachment A, and are both feasible and reliable. 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 manual operator action are diverse from the equipment performing the same function within the DI&C system, such that it is not subject to the same CCF vulnerabilities.

c. The credited SSC is accessible to the operator during the associated event conditions, capable of functioning under the event conditions expected, and of adequate quality, which 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.

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 can propose a new diverse system (e.g., diverse actuation system) as a diverse means to provide the same or a different function credited in the D3 assessment or to mitigate spurious operation due to CCF. If a new system is credited as a diverse means to address potential CCFs, the reviewer should determine whether the application demonstrates that (1) the functions performed by this diverse means are adequate to maintain plant conditions within specified acceptance criteria for the associated DBE, and (2) sufficient diversity exists between this new system and the proposed system so that they are not subject to the same postulated CCF. The reviewer should determine whether the diverse means credited and the digital design used for the proposed system are subject to the same CCF vulnerability. Section 2.6 of NUREG/CR-6303 identifies six diversity attributes and 25 related diversity criteria that NRC reviewers can use to consider whether the new diverse system is adequate to mitigate the CCFs.

The diverse means may be performed by an NSR system if the system is of sufficient quality to

perform the necessary function(s) under the associated event conditions. The reviewer should consider whether the new diverse system is capable of functioning under the event conditions expected and of adequate quality, which 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.

Prioritization

If a new diverse system is implemented, the reviewer should verify that signals to actuate components coming from the different systems are adequately prioritized to ensure the overall defense-in-depth strategy is maintained. 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 over the resources, so safety and protection functions are always carried out. 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 identified below are met, the reviewer should reach a conclusion that using a new diverse system is acceptable. The acceptance criteria are:

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

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

e. 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.

3.3. Consequences of a Common-Cause Failure May Be Acceptable

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

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

Acceptance Criteria

If the acceptance criteria identified below are met, the reviewer should reach a conclusion that the application provides adequate information to show that consequences of potential CCFs of a proposed system or portions of a proposed system are acceptable. The acceptance criteria are:

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

b. For each AOO in the design basis occurring concurrent 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 violation of the integrity of the primary coolant pressure boundary.

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

4. Manual System Level Actuation and Indications to Address Position 4

Position 4 states that an 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. Critical safety functions are defined in Section B.1.2 of this BTP.

RG 1.62 outlines important design criteria for I&C equipment used by plant operators for the manual initiation of protective actions.

The reviewer should consider whether displays and manual controls provided to meet Position 4 are not subject to the same CCF vulnerability 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 did not credit the same digital platform or analog technology for Position 3 (e.g., for mitigating DBEs). Position 4 specifies that the MCR displays and controls shall be independent and diverse from the digital platform or analog technology identified for Positions 1 and 3.

If not subject to that CCF vulnerability, the applicant may credit some or all of these displays and manual controls to meet Position 4 as the diverse means called for under Position 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 Position 3, they may also be credited for Position 4. However, if the diverse means credited for Position 3 is not located in the MCR, then it would not be sufficient to address Position 4.

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

Acceptance Criteria

If the acceptance criteria identified below are met, the reviewer should reach a conclusion that the manual controls and supporting displays conform to Position 4. The acceptance criteria are:

a. Proposed manual actions credited to accomplish safety functions that would otherwise have been accomplished by automatic safety actions are both feasible and reliable, as demonstrated through a human factors analysis, such as the one described in Chapter 18 of this SRP. Section 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 following critical safety parameters: reactivity, core heat removal, reactor coolant inventory. The minimum inventory also allows the operator to initiate and monitor the status of containment isolation and containment integrity.

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

d. The manual controls for these critical safety functions are at the system- or

division-level and 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, the quality and reliability of the equipment is adequate to support the manual operator action during the associated event condition. Quality of this equipment 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.

f. The displays and controls are independent and diverse from the equipment performing the same functions within the safety-related DI&C systems. These displays and controls are no 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 the review described in earlier sections, the NRC staff reviewer should also work with NRC staff in other discipline areas to identify other disciplinary areas that may be affected by CCFs. The technical staff should review the following for potential inter-disciplinary concerns:

a. An 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 vulnerabilities (residual risks) to potential CCFs.

- 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 NRC staff should review the information provided to demonstrate the effectiveness of the diverse means, including assessment from HFE analysis associated with manual operator action if used as a diverse means.

- The results of any consequence analysis that has been performed by the applicant for CCFs that have not been eliminated from further consideration, mitigated using diverse means, or justified as being acceptable. Such an analysis should demonstrate that consequences of a CCF are within acceptable limits for each AOO and PA.

c. For systems that the applicant has not assessed for CCF, information that shows 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 Position 4, design information for a proposed system which shows that controls and displays:

- have been provided in the MCR to perform manual system or division level actuation of critical safety functions.
- are independent and diverse from the equipment performing the same functions within the proposed DI&C system, such that they are not subject to the same CCF as the proposed system.
- have sufficient quality to support the manual operator action during the associated event condition 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. While performing 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 other equipment or software not included in the block. A block can also be a software macro or subroutine, such as a voting block or a proportional-integral-derivative (block, used by multiple functional applications. Systems or components represented as a block may not show the inner workings of the block.

Examples of typical 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 D3 assessment describes the proposed DI&C system or component's diversity between blocks. When considering the effects of a postulated CCF, the diverse blocks can be assumed to function as designed. This includes the functions of blocks that act to prevent or mitigate consequences of the CCF under consideration.

6.2. Documentation of Assumptions

The staff 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 staff 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. Coordination with the NRC staff organization responsible for the review of reactor systems is necessary in reviewing these analyses.

6.4. Identification of Alternative Mitigation Capability

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

When manual operator action is cited as the diverse means for response to an event, the staff reviewer should verify that the applicant's HFE analysis demonstrates that this action is both feasible and reliable, such as through the process described in SRP Chapter 18. This review should include coordination with the organization responsible for the review of human-system interfaces for any credited diverse manual operator action.

6.5. Justification for Not Correcting Specific Vulnerabilities

The reviewer should consider whether justification was provided in the application for not correcting any identified vulnerabilities that were unresolved by other aspects of the application. Such justification might include, for example, design attributes (e.g., redundancy, diversity, independence) and the inclusion of diverse actuation or mitigation capability. This justification might also include previously NRC-approved credited manual operator actions in the licensing basis to address AOOs or PAs. Staff may review the justifications on a case-by-case basis. For example, applicants may potentially credit the ability of plant operators to identify system leakage using the plant leak detection system prior to the onset of a large break pipe rupture. Justification for the crediting of such manual operator actions could be used with appropriate analysis of site-specific factors such as pipe configuration and design, piping fracture mechanics, leak detection system capabilities, and detailed manual operator actions and procedures, as appropriate. The reviewer should consider whether a multi-disciplinary review in cooperation with other NRC staff is necessary to review the justifications provided in the application.

C. REFERENCES

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

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

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

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

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

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

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

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

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

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

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

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

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

14. U.S. Nuclear Regulatory Commission, “Transient and Accident Analysis,” NUREG 0800,

SRP Section 15.0.

15. U.S. Nuclear Regulatory Commission, “Human Factors Engineering,” NUREG 0800, SRP Section 18.0, Revision 3, December 2016

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

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

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

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

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

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

22. 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.

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

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

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

26. 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
To be determined when this document is final.

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 IN DIGITAL SAFETY SYSTEMS

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

The main purpose of this update is to provide clarification on sections of the guidance that proved challenging to implement based upon feedback received by internal and external stakeholders. This update improves readability and the flow of information such that it is clear to the reader that there is an established process for analyzing potential vulnerabilities to common-cause failures resulting from improper implementation of digital technology, in particular within software or software-based logic. This update clarifies the scope of applicability for all users and clearly states the applicability of this guidance to the change process in Title 10 of the *Code of Federal Regulations* (10 CFR) 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. This is in addition to clarifying specific areas of guidance such as diversity and testing, and the addition of both the concepts of alternative methods and qualitative assessment along with supporting failure analysis as means that can be employed to address common-cause failures.