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 ~~HAZARDS~~ DUE TO LATENT ~~SOFTWARE~~DESIGN DEFECTS IN DIGITAL ~~INSTRUMENTATION AND CONTROL~~SAFETY SYSTEMS

## REVIEW RESPONSIBILITIES

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

Secondary – ~~Organization~~Organizations responsible for the review of reactor and containment

~~Draft~~ Revision 8 – ~~January~~December 2020

USNRC STANDARD REVIEW PLAN

This Standard Review Plan, (SRP), NUREG-0800, has been prepared to establish criteria that the U.S. Nuclear Regulatory Commission (NRC) staff responsible for the review of applications to construct and operate nuclear power plants intends to use in evaluating whether an applicant/licensee meets the NRC's regulations. The ~~Standard Review Plan~~SRP is not a substitute for the ~~NRC's~~NRC's regulations, and compliance with it is not required. However, an applicant is required to identify differences between the design features, analytical techniques, and procedural measures proposed for its facility and the SRP acceptance criteria, and to evaluate how the proposed alternatives to the SRP acceptance criteria provide an acceptable method of complying with the ~~NRC~~NRC's regulations.

The ~~standard review plan~~SRP sections are numbered in accordance with corresponding sections in ~~Regulatory Guide~~ RG 1.70, ""Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants (LWR Edition~~)~~."). Not all sections of ~~Regulatory Guide~~RG 1.70 have a corresponding review plan section. The SRP sections applicable to a combined license application for a new light-water reactor (LWR) are based on ~~Regulatory Guide~~ RG 1.206, ""Combined License Applications for Nuclear Power Plants (LWR Edition~~)~~."),"

These documents are made available to the public as part of the NRC's policy to inform the nuclear industry and the general public of regulatory procedures and policies. Individual sections of NUREG-0800 will be revised periodically, as appropriate, to accommodate comments and to reflect new information and experience. Comments may be submitted ~~electronically~~ by ~~e~~mail to ~~NRO~~NRR, SRP@nrc.gov.

Requests for single copies of SRP sections (which may be reproduced) should be made to the U.S. Nuclear Regulatory Commission, Washington, DC 20555, Attention: Reproduction and Distribution Services Section~~, or~~; by fax to (301) 415-2289; or by ~~e~~mail to DISTRIBUTION@nrc.gov. Electronic copies of this section are available through the NRC's public Web site at http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr0800/, or in the NRC's Agencywide Documents Access and Management System (ADAMS), at http://www.nrc.gov/reading-rm/adams.html, under Accession No. ~~ML19256B502~~ MLXXXXXXXXX.

**Style Definition:** Heading 4: Font: Arial, 11 pt, Not Bold, Underline, Indent: Left: 0", Hanging: 0.5", Space Before: 0 pt, After: 0 pt, Don't add space between paragraphs of the same style, Outline numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.06" + Indent at: 0.31", Don't keep with next

**Style Definition** ... [3]

**Style Definition** ... [2]

**Style Definition** ... [1]

**Formatted:** Space Before: 0 pt

**Formatted:** Indent: Left: 0", Hanging: 1"

**Formatted:** Underline

**Formatted:** Underline

**Formatted:** Underline

**Formatted:** Underline

**Formatted:** Underline

**Formatted:** Underline

**Formatted:** Underline

**Formatted:** Highlight

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

## A. BACKGROUND~~-~~

Digital technology offers significant operational and maintenance benefits for I&C systems of nuclear power plants (NPPs). Digital instrumentation and control (DI&C) systems consist of both hardware components and logic elements (e.g., software). Hardware components in DI&C systems are susceptible to failures similar to those considered for analog systems. In this guidance, the term "software" refers to software, firmware,[1] and logic developed from software-based development systems (e.g., hardware description language programmed devices). ~~Common~~

DI&C systems or components are vulnerable to common-cause failures (CCFs) ~~have been identified as a type of hazard that digital I&C (DI&C) systems could be more susceptible to~~ due to ~~the ability to integrate design functions using DI&C technology and its inherent complexity compared to analog technologies. DI&C systems or components can be vulnerable to a CCF due to~~ latent design defects in active hardware ~~or to latent defects in the~~components, software, or software~~-~~based logic.[2] A CCF occurs when multiple (usually identical) systems or components fail due to a shared cause.[3] Latent design defects are errors in the design of the DI&C system or component that can remain undetected despite rigorous design-basis development, verification, validation, and testing processes. Certain events, unexpected external stresses, or plant conditions can trigger latent design defects ~~in hardware, software, or~~

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

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

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

system components within redundant portions (e.g., safety divisions[4]) of a safety-related system can be triggered by an event or condition and designed to perform safety functions and thus lead to a systematic fault. A CCF hazard[5] (e.g., failure.

CCFs can have two different effects: (1) they can cause a loss of the capability to perform a safety function) or can result from the occurrence of suchinitiate a systematic fault during a design-basis event (DBE). This BTP is focused on addressing CCF hazards resulting from systematic faults caused by latent defects in the software or software-based logic.[6]

A CCF of a DI&C system or component can also plant transient, or (2) they can initiate the operation of a safety-related function or other design functions without a valid demand or can result incause an erroneous (i.e., spurious) system actions. These conditions areaction. The latter is typically referred to as "spurious operations," but the term can be used interchangeably with the term" or "spurious actuation." For this BTP, the term "spurious operations" is used. 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 NUREG-0493, "A Defense-in-Depth and Diversity Assessment of the RESAR-414 Integrated Protection System," issued March 1979, the U.S. Nuclear Regulatory Commission (NRC) staff documented a defense-in-depth and diversity (D3) assessment of a digital computer-based reactor protection system (RPS) in which defense against software CCF, which resulted in loss of a safety function during a DBE, was based upon an approach using a specified degree of system separation between echelons of defense. The RESAR-414 RPS consisted of the reactor trip system (RTS) and the engineered safety features (ESF) actuation system. Subsequently, in SECY-91-292, "Digital Computer Systems for Advanced Light-Water Reactors," dated September 16, 1991, the NRC staff discussed its concerns about CCF hazards in digital systems used in nuclear power plants (NPPs).

As a result of reviews of applications for certification of evolutionary and advanced light-water reactor designs using DI&C systems, the NRC staff documented its position regarding vulnerabilities to CCF hazards in DI&C systems and D3 in Item II.Q of SECY-93-087, "accordance with Commission direction in the staff requirements memorandum (SRM) on SECY-93-087, "SECY-93-087—Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," dated April 2, 1993. The Commission subsequently modified this position in Item 18 of the associated staff requirements memorandum (SRM) on SECY-93-087, dated July 21, 1993, in which the Commission indicated that CCF hazards of a DI&C system are considered beyond design-basis events.

The NRC staff provided plans to the Commission to clarify the guidance associated with

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

~~addressing CCF hazards of DI&C systems in SECY-18-0090, "Plan for Addressing Potential Common Cause Failure in Digital Instrumentation and Controls," dated September 12, 2018. This SECY paper documented the NRC staff's evaluation of the SRM on SECY-93-087. The staff concluded that the SRM provides adequate flexibility for regulatory modernization activities that support near-term DI&C implementation. SECY-18-0090 outlines five guiding principles to ensure consistent application of the direction provided in the SRM on SECY-93-087. These principles provide a framework for addressing CCF hazards in DI&C systems using a graded approach based on the safety significance of the DI&C system. In SECY-18-0090, the NRC staff committed to incorporating these guiding principles into the NRC staff's review guidance.~~

~~In summary, while the NRC~~ 1993, the staff considers CCF ~~hazards due to software~~ in DI&C systems to be ~~beyond~~a beyond-design-basis event. The likelihood of occurrence of these failures cannot be predicted through traditional design ~~basis, the application should include an evaluation of CCF hazards due to software in DI&C systems and should verify that the plant is protected from the~~analysis methods, but their effects ~~of these CCF hazards. In addition, the application should include an evaluation of sources of this CCF hazard that can result in spurious operations, some of which may be considered within the design basis, as discussed later in this BTP.~~and consequences can be addressed through other methods, such as best estimate methods.

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

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

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

RTS, the ESFAS, and the reactor monitoring and indication systems as individual echelons of defense.

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

- SRP Appendix 7.0-A, "Review Process for Digital Instrumentation and Control Systems," and BTP 7-21, "Guidance on Digital Computer Real-Time Performance," provide guidance on real-time deterministic processing.
- Item B.3.1 of Table 2 and Item C.7 of Table 3 in SRP Section 13.6.6, "Cyber Security Plan," provide guidance on control of access.
- RG 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," provides guidance on measures protecting against undesirable acts (e.g., tampering with software code or logic) that can compromise the safety system.
- RG 5.71, "Cyber Security Programs for Nuclear Facilities," provides guidance on protecting digital computers and communication systems and networks against cyberattacks.
- BTP 7-17, "Guidance on Self-Test and Surveillance Test Provisions," provides guidance on self-test features.

Over the years, the U.S. Nuclear Regulatory Commission (NRC) staff has approved applications ~~with numerous~~that use various design features to address CCF vulnerabilities in DI&C systems. Some of these use multiple design solutions~~, and in some cases, multiple design solutions for~~ within different parts of a single DI&C system~~, to address CCF hazards in DI&C systems. During~~. In reviewing these ~~reviews~~applications, the ~~NRC~~ staff has ~~observed that~~ evaluated several different solutions that successfully address CCF vulnerabilities. Consequently, the staff recognizes that there may be ~~used to address CCF hazards, and that one standard~~no single solution ~~may not be applicable~~that applies to all DI&C systems. ~~This BTP provides guidance for reviewing the design and analysis for addressing CCF hazards due to latent software defects in DI&C systems.~~

**Formatted:** Highlight

## 1. Regulatory Basis

**Formatted:** Heading 4, No bullets or numbering

The regulations listed below may not ~~necessarily~~ apply to all applicants. ~~The~~Their applicability ~~of these requirements is determined by~~depends on the plant-specific licensing basis and any

proposed changes to the licensing basis ~~in~~ 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), "Protection and Safety Systems,") requires compliance protection systems to be consistent with the plant-specific licensing basis or IEEE Std 603-1991 and the correction sheet dated January 30, 1995.~~

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

- ~~For applications for construction permits (CPs), operating licenses (OLs), combined licenses (COLs), standard design approvals (SDAs), design certifications (DCs), filed after May 13, 1999, 10 CFR 50.55a(h) requires compliance~~ to comply with IEEE Std 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," and with the IEEE Std 603-1991 correction sheet dated January 30, 1995.

- ~~IEEE Std 603-1991, Clause 5.6.3, requires, in part, that "safety system design shall be such that credible failures in and consequential actions by other systems, as documented in [Clause] 4.8 of the design basis, shall not prevent the safety systems from meeting the requirements of this standard." IEEE Std 603-1991, Clause 4.8, requires, in part, that the safety-related system design bases shall document "[t]he conditions having the potential for functional degradation of safety system performance and for which provisions shall be incorporated to retain the capability for performing the safety functions (for example, missiles, pipe breaks, fires, loss of ventilation, spurious operation of fire suppression systems, operator error, failure in non-safety-related systems)." These two clauses provide the basis for requiring licensees of plants licensed under IEEE Std 603-1991 to address the potential for spurious operation of safety-related components and components that are NSR.~~

- ~~GDC 22, "Protection System Independence," requires, in part, that the protection system design shall ensure "~~For NPPs with CPs issued between January 1, 1971, and May 13, 1999, 10 CFR 50.55a(h) requires protection systems to comply with IEEE Std 279-1968, "Proposed IEEE Criteria for Nuclear Power Plant Protection Systems"; IEEE Std 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations"; or IEEE Std 603-1991 and the correction sheet dated January 30, 1995.

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

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

  > The protection system shall be designed to assure that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function~~...~~, or shall be demonstrated to be acceptable on some other defined basis. Design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protection function~~." GDC 22 provides the regulatory basis for the requirement to address CCF hazards and for requiring the use of design techniques, such as functional diversity or diversity in component design, to prevent the loss of the protection function.~~.

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

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

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

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

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

**Formatted:** Normal, Indent: Left: 1", Right: 0.5", No bullets or numbering

for nuclear power facilities.

- The regulations in 10 CFR Part 100, "Reactor site criteria," Subpart A, "Evaluation Factors for Stationary Power Reactor Site ~~Criteria," provides guideline values for fission product releases from NPPs licensed to operate prior to~~ Applications Before January ~~1~~0, 1997~~,~~, and for ~~which the licensee has voluntarily implemented an alternative source term under the provisions~~Testing Reactors," apply to holders of ~~10 CFR 50.67, "Accident Source Term." These guideline values can be~~ and applicants for OLs whose CPs were issued before January 10, 1997, and required the CP applicant to assume a fission product release from the core for use in deriving an exclusion area, a low-population zone, and population center distance. The dose criteria in 10 CFR 100.11(a) are commonly referred to as ~~the~~ "site dose guideline values" and provide ~~the~~reference values for site evaluation, which can also be used as acceptance criteria for ~~radiological release limits to bound~~evaluating the adequacy of DI&C design by considering the consequences of a CCF ~~hazards~~ concurrent with a design-basis event (DBE~~.~~).

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

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

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

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

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

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

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

2. Relevant Guidance

The following documents provide useful guidance in the evaluation of possible CCFs in digital

Formatted: Indent: First line: 0"

Formatted: Indent: Hanging: 0.5", Bulleted + Level: 1 + Aligned at: 0.25" + Indent at: 0.5"

Formatted: Indent: Left: 0", First line: 0"

Formatted: Heading 4, No bullets or numbering

Formatted: Underline

safety system designs:

- NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems," issued December 1994, summarizes several diversity and defense-in-depth (D3) analyses performed after 1990 and. It presents a method for performing such analyses. Within NUREG/CR-6303, ananalyzing proposed DI&C systems to identify vulnerabilities to common-mode failures[7] and to confirm that the design incorporates adequate D3 strategies to address them. This analysis method is presented that postulates common-mode failures[8] that could occur within digital RPSsreactor protection systems and determines what portions of a design need to implement additional D3 measures to address such failures. -

- NUREG/CR--7007, "Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems," issued December 2008, provides guidance anddiversity strategies after a D3 assessment has been performed and it is determined that diversity to mitigate CCF vulnerabilities in a given safety-related system is needed for mitigating potential vulnerabilities that can lead to for which a D3 assessment has shown a CCF hazard.need for greater diversity. NUREG/CR-7007 identifies and develops a baseline set of diversity criteria that may constitutebe appropriate mitigating diversity strategies to addressfor addressing potential vulnerabilities to CCF hazardsCCFs. While this NUREG describes a method for quantitatively assessing the amount of diversity in a system, this method has not been benchmarked and should not be used as the sole basis for justifying adequate diversity.

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

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

- Generic Letter (GL) 85-06, "Quality Assurance Guidance for ATWS Equipment That Isis Not Safety-Related," dated April 16,- 1985, provides quality assurance guidance for anticipated transient without scram (ATWS) equipment that is not safety related (NSR.-- The guidance within this generic letter ). GL 85-06 describes methods that may be used to demonstrate theestablish quality ofassurance measures for equipment that is NSR and credited for providing the diverse means to mitigate a CCF hazardpotential CCFs.

- RG 1.62, "Manual Initiation of Protective Actions," describes a method that the staff

Formatted: Strikethrough

Formatted: Indent: First line: 0"

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

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

considers acceptable for use in complying with the NRC's regulations concerning the means for manual initiation of protective actions provided (1) by otherwise automatically initiated safety systems or (2) as a method diverse from automatic initiation.

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

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

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

- NUREG-0800, SRP Section 7.8, "Diverse Instrumentation and Control Systems," describes the review process and additional acceptance criteria for diverse I&C systems provided to protect against CCF hazardsthe 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 actionactions as a diverse means of coping with anticipated operational occurrences (AOOs) and postulated accidentsPAs that are concurrent with a CCF hazard due to latent design defects that disablesdisable a safety function credited in the safety analysis report (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 (1) I&C safety systems proposed (1) in requests for license amendments as modifications that require a license amendment to be implemented, andlicensed NPPs, or (2) in applications for CPs, OLs, COLs, DCs, SDAs, and MLs. This BTP isdoes not applicableapply to proposed modifications performed under the change process in 10 CFR 50.59, "Changes, Teststests and experiments."

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

Formatted: Widow/Orphan control

Formatted: Normal

Formatted: Heading 4, No bullets or numbering

failures in NSR systems.

## 4. Purpose

~~The purpose of this~~This BTP ~~is to provide~~provides the NRC staff with guidance for ~~reviewing an evaluation of (1) a DI&C system's vulnerability to a CCF hazard due to latent defects in the software or software-based logic, (2) any diverse means credited to~~ evaluating an applicant's assessment of the adequacy of D3 for a proposed DI&C system. The applicant performs this D3 assessment to identify and address ~~remaining vulnerabilities to a CCF hazard, and (3)~~potential CCFs in a proposed DI&C system and to evaluate the effects of any ~~unmitigated vulnerabilities to a CCF hazard~~unprevented CCFs on plant safety.

This BTP also provides guidance ~~on implementing a graded approach to address CCF hazards due to latent defects in the software or software-based logic in DI&C systems~~for review of the following:

- the appropriateness of an applicant's chosen methods for performing a D3 assessment, including any categorization of proposed DI&C SSCs based on the safety significance of the ~~system. In this guidance, software includes software, firmware,[9] and logic developed from software-based development systems (e.g., functions they perform~~~~hardware description language programmed devices).~~

~~This BTP is intended to address an applicant's approach to address CCF hazards caused by latent defects in the software or software-based logic. This type of CCF hazard is considered a beyond-design-basis event for structures, systems, and components (SSCs) that employ a robust design process to reduce the likelihood of design defects. The plant response to these beyond-design-basis events may be analyzed using either conservative or best-estimate methods. However, in integrated DI&C systems, a single random hardware failure can have cascading effects, similar to a CCF hazard (e.g., loss of multiple functions within a safety group, or spurious operation of functions within multiple safety groups). Single random hardware failures with cascading effects are considered DBEs, because random hardware failures are expected during the life of the facility. DBEs should be analyzed using conservative methods to demonstrate that the plant response to these events is bounded by the events in the accident analysis section of the SAR. RG 1.53 provides guidance for the deterministic analysis of single failures in safety-related systems.~~

- ~~This BTP provides guidance for reviewing (1)~~proposed design attributes~~,~~ ~~—~~such as the use of diverse equipment ~~within~~, testing, or NRC-approved alternative methods, including defensive measures, in the design of a system or component ~~to —~~that may eliminate ~~the~~a potential CCF ~~hazard~~ from further consideration~~,~~10 ~~(2)~~

~~[9] 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.~~

[10] ~~The description of~~ Section B.3.1 of this BTP describes how a potential CCF ~~hazard is~~can be eliminated from further consideration ~~is discussed in Section B.3.1 of this BTP~~.

**Formatted:** Heading 4, No bullets or numbering

**Formatted:** List Paragraph, Indent: Hanging: 0.54", Bulleted + Level: 1 + Aligned at: 0.29" + Indent at: 0.54"

**Formatted:** List Paragraph, Indent: Left: 0", Hanging: 0.54"

**Formatted:** Default Paragraph Font, Not Superscript/ Subscript

**Formatted:** Indent: Left: 0", Hanging: 0.5"

- an applicant's use of diverse external equipment, including manual controls and displays, to mitigate a potential CCF ~~hazard, and (3),~~ as well as other measures to ensure conformance with the NRC's position on addressing ~~CCF hazards~~CCFs in DI&C systems as specified in ~~the~~ SRM ~~on~~ SECY-93-087 and SECY-18-0090~~. The objectives of this review are to verify the following:~~

~~- Vulnerabilities to a CCF hazard have been adequately identified and addressed for DI&C systems using a graded approach based on the safety significance of the system.~~

~~- For DI&C systems of high safety significance, an adequate D3 assessment has been conducted and meets the acceptance criteria described in this BTP. An adequate D3 assessment consists of~~

  ~~– An evaluation of vulnerabilities to a CCF hazard due to latent defects in system and the effectiveness of any credited attributes to eliminate the CCF hazard from further consideration;~~

  ~~– Identification of any credited diverse means to mitigate CCF hazards that have not been eliminated from further consideration and the evaluation of the effectiveness of these diverse means; and~~

  ~~– An assessment of the consequences of residual CCF hazards that have not been eliminated from further consideration or mitigated to demonstrate that the consequences remain bounded[11] by the events analyzed in the accident analyses.~~

~~- A qualitative assessment of proposed DI&C systems of lower safety significance obtains results that meet the acceptance criteria within this BTP.~~

This BTP also addresses review of the applicant's assessment of vulnerabilities to a CCF ~~hazard due to latent software defects~~ that can cause ~~the~~a spurious operation ~~of a safety-related component or a component that is NSR, because such~~. It provides the staff with guidance for evaluating applicant analyses of a proposed modification's ability to withstand or cope with CCFs resulting in spurious operations ~~have the potential to put the plant in a condition that has not been previously analyzed in the accident analysis. If these conditions have not been analyzed, then such conditions may not be adequately mitigated by an I&C system. This BTP provides criteria for reviewing an applicant's assessment of CCF hazards of DI&C systems that can result in spurious operation of safety-related components or components that are NSR.~~

## B. BRANCH TECHNICAL POSITION

### 1. Introduction

The overall objective of this BTP is to provide criteria for the staff's evaluation of the

~~[11] The term "bounded" as used in the BTP means that the plant conditions remain within the acceptance criteria of the events analysis in the accident analysis.~~

**Formatted:** List Paragraph, Indent: Left: 0", Hanging: 0.54", Space Before: 11 pt, Bulleted + Level: 1 + Aligned at: 0.29" + Indent at: 0.54"

**Formatted:** Indent: Left: 0", First line: 0"

**Formatted:** Heading 4, Indent: Left: 0", Hanging: 0.5", Outline numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.06" + Indent at: 0.31"

acceptability of the applicant's D3 assessment of proposed DI&C systems.[12]

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

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

The reviewer should consider whether the applicant's assessment has properly identified and addressed CCFs and whether the applicant has incorporated appropriate means to limit, mitigate, or withstand or cope with (i.e., accept the consequences of) possible CCFs and sources of CCF vulnerability that can result in spurious operations.

~~1.1.~~1.1 Four-Point Common-Cause Failure ~~Positions~~Position and ~~Clarification~~Discussion

The foundation of BTP 7-19 is the "NRC position on D3" from ~~the~~ SRM ~~on~~ SECY-93-087, ~~Item 18. The~~ which consists of the four ~~positions stated in the SRM on SECY-93-087 are~~points 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.~~"~~."

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

Formatted: Indent: Left: 0"

Formatted: Heading 5, Indent: Hanging: 0.5", Outline numbered + Level: 2 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Indent at: 0.5"

Formatted: Indent: Left: 0.5", Hanging: 0.5", Right: 0.5"

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. [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. [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 Itemsitems 1 and 3 above.”.[13]

SECY-18-0090 clarifies the application of the Commission’s direction in the above four positions to reduce regulatory uncertainty. In accordance with Position 1 of SRM on SECY-93-087, Item 18, a D3 assessment should be performed. Section B.3 of this BTP provides review guidance and acceptance criteria for a D3 assessment to demonstrate that vulnerabilities to CCF hazards have been adequately addressed. The guiding principles withinin SECY-18-0090 clarify that it is acceptable to use a graded approach the D3 assessment described in point 1 should be commensurate with the safety significance of the proposed DI&C system or component to determine. Section B.2 provides guidance for reviewing an applicant’s safety-significance determinations, if any are used, and Section B.3.1 contains guidance for reviewing an applicant’s use of those determinations in the D3 assessment. Section B.2 also covers the review of an applicant’s determination that a D3 assessment is not necessary, based on a failure analysis.
Point 2 uses the degree of rigor that is necessary to address CCF hazards. This graded approach is described in Section B.2.1 of this BTP.

The term “best estimate methods” in Position 2 is,” but this term is somewhat out of date; the same methods are now referred totypically described as methods usingthat use “realistic assumptions,” which are defined as the initial plant conditions corresponding to the onset of the

Formatted: Space Before: 11 pt

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

event being analyzed. ~~Initial plant event conditions include~~Point 2 also includes acceptance criteria that are less conservative than the acceptance criteria defined in the updated final safety analysis report (FSAR) for the applicable limiting events within the design basis. Initial plant event conditions include, but are not limited to, the following:

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

~~The guiding principles within~~ SECY-18-0090 ~~clarify~~clarifies that, in addition to ~~"best estimate~~ the methods~~" (i.e., "~~ using realistic assumptions~~")~~ identified in ~~Position~~point 2 ~~of SRM on SECY-93-087, Item 18~~, the D3 assessment can be performed using a design-~~-~~basis analysis~~ (i.e.,~~. The key distinction is that a design-basis analysis uses conservative ~~methods). Thus, when performing the D3 assessment, it is acceptable to use either realistic~~ assumptions ~~to analyze the plant response to DBEs, or the conservative assumptions on which the accident analysis based. Each~~. Reviewers should consider whether each event analyzed ~~within~~in the accident analysis ~~should be~~is evaluated in the D3 assessment independently. For example, if the initiating event is the loss of offsite power, the assessment does not need to assume another concurrent DBE.

If the D3 assessment shows that a postulated CCF could disable a safety function ~~(i.e., become a CCF hazard),~~, then ~~Position~~point 3 directs ~~the assessment to identify an existing~~ that a diverse means ~~or add a diverse means~~ be provided to perform ~~the~~that safety function or a different function. The diverse means may already exist in the facility or may be installed in connection with the DI&C modification. The diverse means may ~~be~~comprise NSR equipment ~~that is NSR~~, together with a documented basis that ~~the diverse means~~ this equipment is of sufficient quality and ~~unlikely to be subject~~is not vulnerable to the same CCF ~~hazard. While the enclosure to Generic Letter 85-06 provides~~. Methods for demonstrating sufficient quality ~~assurance guidance for ATWS equipment, this guidance can also be applied to equipment that is NSR credited as the diverse means for addressing CCF hazards.~~include application of the alternative treatment provided in 10 CFR 50.69(d)[14] and quality controls or measures developed in accordance with GL 85-06. SECY-18-0090 clarifies that ~~use of~~ either automatic or manual actuation within an acceptable time frame is ~~an acceptable~~a permissible diverse means of ~~diverse~~ actuation. ~~SECY-18-0090 also specifies that if~~If the D3 assessment demonstrates that a ~~CCF hazard, when evaluated in the accident analysis~~ possible CCF can be reasonably mitigated ~~through~~by other means (~~such as with current~~e.g., using other installed systems), a diverse means that performs the same or a different function may not be needed. For example, an ATWS system may be credited as the diverse means of tripping the reactor, provided it is not ~~subject~~vulnerable to the same CCF ~~hazard~~ that ~~disabled~~could disable the safety function.

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

If a diverse means is part of a safety--related system, it ~~would~~is then ~~be~~ subject to ~~meeting~~the divisional independence requirements in IEEE Std 603-1991, Clause 5.6.1, which is incorporated by reference ~~pursuant to~~into 10- CFR- 50.55a, "Codes and ~~Standards."~~ standards." If the diverse means is NSR, then the requirements in IEEE Std 603-1991, Clause 5.6.3- ~~requirements~~ , for separation and independence between safety--related systems and NSR systems ~~that are NSR should be met~~apply.

~~Position~~Point 4 directs the inclusion of a set of displays and manual controls ~~("safety" or "non-safety")~~ in the main control room (MCR) that is independent of and diverse from ~~any vulnerability to a CCF hazard identified within~~ the "safety computer system" discussed in ~~Positions~~points 1 and- 3 ~~above and meets~~ .[15] The reviewer should determine whether this set of displays and manual controls provides for divisional independence ~~requirements~~ as applicable ~~for~~to the specific design implementation. ~~While the SRM on SECY-93-087 uses the terms "safety" and "non-safety," these terms in context refer to safety-related and NSR SSCs, respectively.~~ Depending on the design, these displays and controls should provide manual system- or ~~divisional~~ division-level actuation and control of equipment to manage the "critical safety functions" (see Section B.1.2). ~~Further~~[16]

Furthermore, if not ~~subject~~vulnerable to the same CCF as the proposed safety--related DI&C system, some of ~~these~~the displays and manual controls from ~~Position~~point 4[17] may be credited as all or part of the diverse means provided to address ~~Position~~point 3.

The ~~Position~~point 4 phrase "safety computer system identified in ~~Items~~items 1 and- 3 ~~above~~" refers to a safety--related DI&C system that is credited for mitigating an AOO or ~~postulated accident~~PA in the accident analysis. Typically, the automatic safety--related I&C system is credited, but for some events, manual safety--related controls are ~~the ones~~ credited.

~~The four positions from the SRM on SECY-93-087, acknowledge that DI&C system development errors (i.e., latent defects) are a credible source of CCF hazards. Generally, DI&C systems containing software or logic cannot be fully tested except for very limited cases, nor can their failure modes be completely predicted because software does not have a physical manifestation that limits its behavior. Therefore, DI&C systems may be vulnerable to CCF hazards if either (1) identical system designs and identical copies of the software or software-based logic are present in redundant divisions of safety-related systems, or (2) previously separated functions have been integrated into a single DI&C system. Also, some errors, such as those labeled as "software design errors," normally result from errors in the higher-level requirements (e.g., system requirements or design specifications), in which the system design misrepresents the actual process. As used in this BTP, terms such as "higher-level requirements" do not refer to NRC regulatory requirements but to system or component~~

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

[16] SECY-18-0090 did not elaborate on point 4.

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

~~design or operating characteristics that are relied upon to accomplish the stated system or component functions. Throughout this BTP, context indicates whether requirements are NRC regulatory requirements.~~

~~SECY-18-0090 recognizes that, although significant effort has been applied to the development of highly reliable DI&C systems, some residual faults may remain undetected within a system and could result in CCF hazards that can challenge plant safety. This includes CCF hazards that result from loss of the safety function or those caused by spurious operation of a safety function or other design function. To address these CCF hazards, the NRC staff should verify that for each event analyzed in the accident analysis section of the SAR, the application has:~~

- ~~Identified vulnerabilities to CCFs due to a design or implementation defect in a DI&C system and evaluated the impacts of these postulated CCFs to safety functions or other design functions to determine whether these postulated CCFs can lead to a hazard;~~
- ~~Demonstrated that a CCF hazard due to these residual defects has been either adequately prevented through use of appropriate measures (e.g., diversity within the design, testing, and defensive measures) or mitigated through use of a diverse means; and~~
- ~~Assessed the ability of the overall plant design (e.g., I&C systems, mechanical systems, and manual operator action) to maintain plant safety, using conservative or "best estimate" methods, for those CCF hazards that have not been shown to be prevented or mitigated.~~

~~1.2.~~1.2 Critical Safety Functions

**Formatted:** Heading 5, Indent: Hanging: 0.5", Outline numbered + Level: 2 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Indent at: 0.5"

~~In the revised~~ SECY-93-~~087, Item II.Q, included with the SRM, the NRC staff~~0087 identified the following critical safety functions to be managed from the MCR ~~per Position~~ in accordance with point 4 ~~of this SRM~~:

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

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

**Formatted:** Underline

~~2.~~1. ~~Graded Approach~~Safety Significance and ~~Level of Integration for Addressing Common Cause~~ Effects of Failure

**Formatted:** Heading 4, Indent: Left: 0", Hanging: 0.5", Outline numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.06" + Indent at: 0.31"

**Formatted:** Widow/Orphan control

## 2.1. Graded Approach for Categorizing Digital Instrumentation and Control Systems

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

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

| | **Safety-Related** | **Not Safety-Related** |
|---|---|---|
| **Safety Significant**<br>A significant contributor to plant safety | **A1 DI&C SSCs**<br><br>Relied upon to initiate and complete control actions essential to maintain plant parameters within acceptable limits established for a DBE.<br><br>**or**<br><br>Failure could directly lead to accident conditions that may cause unacceptable consequences (i.e., exceeds siting dose guidelines for a DBE) if not mitigated by other A1 systems.<br><br>**Application should include a D3 assessment as described in Section B.3** | **B1 DI&C SSCs**<br><br>Directly changes the reactivity or power level of the reactor, or affects the integrity of the safety barriers (fuel cladding, reactor vessel, or containment).<br><br>**or**<br><br>Failure may result in unacceptable consequences to plant safety due to integration of multiple control functions into a single system.<br><br>**Application should include a qualitative assessment as described in Section B.4** |

| | | |
|---|---|---|
| **Not Safety Significant**<br>Not a significant contributor to plant safety | **A2 DI&C SSCs**<br><br>Provides an auxiliary or indirect function in the achievement or maintenance of plant safety.<br><br>**or**<br><br>Maintains the plant in a safe shutdown state after the plant has reached initial safe shutdown state.[18]<br><br>**Application should include a qualitative assessment as described in Section B.4** | **B2 DI&C SSCs**<br><br>Does not have a direct effect on reactivity or power level of the reactor or affect the integrity of the safety barriers (fuel cladding, reactor vessel, or containment).<br><br>**and**<br><br>Failure does not have consequences to plant safety or whose failure can be detected and mitigated with significant safety margin.<br><br>**Application may need to include a qualitative assessment as described in Section B.4** if the proposed design could introduce conditions[19] that have not been previously analyzed in the SAR. |

This section provides guidance to reviewers on implementing Principle 3 in SECY-18-0090, which explains that a D3 assessment should be "commensurate with the safety significance of the system" and "

For example, an assessment of CCF hazards for a digital RTS would be expected to be more rigorous than an assessment of CCF hazards for a safety-related MCR Heating, Venting, and Air Conditioning (HVAC) chiller. While the HVAC chiller is a safety-related system that maintains certain temperature and humidity in the MCR for equipment and personnel to operate properly, a failure of this system is not as significant as the failure of the RTS because operators will have operating procedures or diverse means to control temperature and humidity and will shut down the plant, if necessary.

Risk insights in terms of safety consequences from site-specific probabilistic risk assessments (PRAs) can be used to support the safety-significance determination in categorizing the DI&C system. Use of such risk insights should be an input to an integrated decision-making process for categorizing the proposed DI&C system. The application should document the basis for categorizing the proposed DI&C system, including any use of risk insights.

The graded approach presented in Table 2-1 is consistent with SECY-18-0090, which states that "an analysis may not be necessary for some low-safety-significance I&C systems whose failure would not adversely affect a safety function or place a plant in a condition that cannot be reasonably mitigated." 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.

Formatted: Widow/Orphan control, Tab stops: Not at 0.13"

## 2.1 Safety-Significance Determination

For the purposes of this BTP, a safety-significant function is one whose degradation or

Formatted: Right: 0.5"

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

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

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

System Integration and Interconnectivity

System integration and interconnectivity ~~among the categories identified in Table 2-1~~ can introduce additional CCF vulnerabilities ~~to CCF hazards.~~. If there is integration (e.g., through combined design functions, shared resources, or digital interconnectivity~~) among A1 systems or among A1 and systems in the other three categories, then the assessment for the~~ ), the system should be assessed using the methods appropriate for the highest safety-significance SSC that is integrated or interconnected. The reviewer should consider whether the applicant included a clear description of the proposed ~~A1 system should consider the CCF hazards of the integrated~~ DI&C system or component that identifies (1) shared resources, (2) interconnection with other systems, and (3) whether the modification could reduce the redundancy, diversity, separation, or independence of systems described in the facility's SAR. Reductions in independence, separation, diversity, or redundancy can adversely affect the defense-in-depth of a plant.

The reviewer should also determine whether the assessment of the most safety significant SSCs considers the vulnerability to CCF resulting from failures within the integrated or interconnected system and the consequences of ~~these~~a CCF ~~hazards~~ that could affect the proper operations of the integrated or interconnected ~~A1~~ systems. For example, ~~if~~ a digital protection system ~~includes~~may include controllers for performing reactor trip and engineered safety feature (ESF) logic, as well as safety~~-related~~ control functions (e.g., auxiliary feedwater level control~~), and~~). If the reactor trip or ESF initiation signal ~~only~~ in such a system reaches the final actuation device ~~via~~only through the equipment that performs ~~these~~ safety~~-related~~ control functions, then the ~~categorization of~~reviewer should determine whether all the ~~equipment~~SSCs in that pathway ~~should be A1. A~~have been assigned to the highest safety significant SSC category. In this example, the reviewer should determine whether the D3 assessment ~~should~~

Formatted: Not Strikethrough

Formatted: List Paragraph

Formatted: Normal, Indent: Left: 0", Tab stops: Not at 0.13"

~~be performed in accordance with the guidance in Section B.3 on these interconnected or integrated systems. In performing this assessment, the criteria in Sections B.3.1 through B.3.3 for an A1 system apply to~~for these interconnected or integrated systems~~.~~ meets the criteria in Sections B.3.1–B.3.3 for D3 assessments of high safety-significant SSCs.

Formatted: Normal, Indent: Left: 0", Tab stops: Not at 0.13"

Acceptance Criteria for Safety-Significance Determinations:

NRC technical reviewers should find an applicant's safety-significance determination acceptable if it reasonably conforms to the criteria below. If the applicant uses risk insights (e.g., from a site-specific PRA) to demonstrate that an SSC is less safety-significant than these criteria would indicate, the staff should review these on a case-by-case basis. The following acceptance criteria applies:

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

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

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

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

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

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

- They provide an auxiliary or indirect function in the achievement or maintenance of a safety-related function.
- They perform an NSR design function that contributes significantly to plant safety.
- They are capable of directly changing the reactivity or power level of the reactor

and their failure could initiate an accident sequence or could adversely affect the integrity of a safety barrier (i.e., fuel cladding, reactor vessel, or containment).

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

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

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

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

~~3.~~2.2 Using Safety Significance to Determine Whether a Diversity and Defense- in- Depth ~~(D3)~~ Assessment Is Necessary

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

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

Acceptance Criteria

~~a proposed A1 system or component to determine whether~~ If the application meets the acceptance criteria identified below, the reviewer should conclude that a D3 assessment is not necessary because a failure analysis demonstrates that failure of the specified SSC cannot adversely affect a safety function or place the plant in a condition that cannot reasonably be mitigated. The acceptance criteria are as follows:

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

Formatted: No underline
Formatted: Heading 5, Indent: Hanging: 0.5", Outline numbered + Level: 2 + Numbering Style: 1, 2, 3, … + Start at: 2 + Alignment: Left + Aligned at: 0.25" + Indent at: 0.5"
Formatted: No underline
Formatted: No underline
Formatted: No underline
Formatted: No underline
Formatted: Normal
Formatted: Tab stops: Not at 0.63"
Formatted: No widow/orphan control, Don't keep with next

- 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.

1. Diversity and Defense-in-Depth Assessment

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

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

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

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

- For each event analyzed in the accident analysis ~~section~~sections of the ~~safety analysis report, the results of~~SAR, evaluate whether the D3 assessment ~~should show~~indicates that CCF vulnerabilities ~~to CCF hazards~~that might result in loss of function have been adequately addressed ~~through any combination of the following:~~

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

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

General Approach

Formatted: List Paragraph, Indent: Hanging: 0.5", Bulleted + Level: 1 + Aligned at: 0.25" + Indent at: 0.5"

Formatted: List Paragraph, Indent: Hanging: 0.5"

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

- The applicant eliminated CCF vulnerabilities from further consideration ~~per~~through any of the ~~criteria~~methods below, either alone or in combination:

  ~~a.~~ using diversity within the DI&C system or component (Section B.3.1~~;~~.1)

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

  – using testing (Section B.3.1.2)

  – using alternative methods (Section B.3.1.3)

  – for low-safety-significance SSCs, using a qualitative assessment and failure analysis (Section B.3.1.4)

- The applicant mitigated consequences of ~~the CCF hazard are acceptable for the associated DBE per the~~ CCF vulnerabilities using one or more of the design techniques below:

  – crediting existing systems (Section B.3.2.1)
  – crediting manual operator actions (Section B.3.2.2)
  – crediting a new diverse system (Section B.3.2.3)

~~c.~~ The applicant analyzed consequences of CCF vulnerabilities and found them to remain within the acceptance criteria ~~within Section B.3.3.~~

- ~~The applicant may elect~~defined in the FSAR or the LAR for the limiting events applicable to ~~apply any combination of the above three methods to the entire A1~~the proposed DI&C system or component (Section B.3.3)

If the applicant used multiple strategies to address CCF vulnerabilities in different portions of a system, then the reviewer should evaluate the applicant's analysis of the ~~A1 system.~~CCF vulnerabilities in each portion and identify how each method was applied. For example, ~~the applicant may show that the CCF hazard has been eliminated for a component within the A1 system and exclude this component when addressing the CCF hazard for the rest of the A1~~ in one portion of the system~~.~~, the applicant might eliminate a CCF from further consideration, while in another portion, the applicant might mitigate the CCF vulnerability using diverse I&C systems.

Spurious Operation as a Result of Common-Cause Failure

The ~~adequacy~~evaluation of potential spurious operations is an important part of the overall D3



**Formatted:** Indent: Left: 0.5", Hanging: 0.5", Space After: 0 pt, Don't add space between paragraphs of the same style, Bulleted + Level: 1 + Aligned at: 0.5" + Indent at: 0.75"

**Formatted:** Default Paragraph Font

**Formatted:** Default Paragraph Font

**Formatted:** Normal

**Formatted:** Default Paragraph Font

**Formatted:** Default Paragraph Font

**Formatted:** Default Paragraph Font

**Formatted:** Default Paragraph Font

**Formatted:** Default Paragraph Font

assessment, including any (1) measures used for a proposed DI&C system to eliminate the CCF hazard from further consideration, (2) diverse means providedensure that spurious operations do not lead to mitigate the CCF hazard, or (3) analysis to show the events with unacceptable consequences.

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

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

*Sources of Spurious Operation*

Spurious operations originating from CCFs due to latent design defects are considered beyond-design-basis events and are within the scope of this BTP.[20] As stated in the background section of this BTP, CCFs should be evaluated in a manner consistent with SRM-SECY-93-087. Therefore, the reviewer may apply the methodologies described in this BTP when evaluating spurious operations resulting from CCFs.

*Spurious Operation and Integrated Systems*[21]

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

When of the evaluating integrated systems, the reviewer should focus primarily on NSR SSCs

Formatted: Normal, Space After: 0 pt, No bullets or numbering, Keep with next

Formatted: No widow/orphan control

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

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

that are integrated with safety-related SSCs. This is because safety-related SSCs have particular regulatory requirements (e.g., for independence and quality) that separately address CCF ~~hazard are acceptable for each DBE, should be justified in the application and explicitly~~vulnerabilities in integrated systems. A secondary focus should be on integration of NSR SSCs that can directly or indirectly affect reactivity (e.g., an NSR rod control system). In some cases, an NSR system may be susceptible to failures not analyzed in the design bases. The reviewer should consider whether a CCF of an integrated NSR DI&C system or platform (e.g., a single platform controlling multiple NSR system functions) could result in spurious operation that would have unacceptable consequences. The reviewer should also consider the level of integration between safety and NSR systems as a potential vulnerability to be addressed in the ~~NRC staff's safety evaluation.~~application.[22]

*Staff's Evaluation of Spurious Operation*

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

~~3.1.~~1.1. Means to Eliminate the Potential for Common ~~-~~Cause Failure ~~Hazard~~ from Consideration

**Formatted:** Heading 5, Indent: Left: 0", Hanging: 0.5", Outline numbered + Level: 2 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Indent at: 0.55", Keep with next

Many system design and testing attributes, procedures, measures, and practices can ~~contribute to~~ significantly ~~reducing~~reduce the likelihood of a CCF ~~hazard. However, there are certain design attributes that are sufficient~~. In a D3 assessment, the following methods can be used to eliminate a potential CCF from further consideration ~~a CCF hazard due to a digital design or implementation defect. These attributes include~~: (1) demonstration of adequate diversity within the DI&C system or component, (2) ~~testability~~ testing, and (3) ~~defensive measures~~ other NRC-approved alternative methods within the ~~design. Although these attributes do not eliminate the CCF hazard completely,~~ application. In addition, for SSCs with low safety significance, a qualitative assessment and failure analysis showing that the ~~residual risk for a CCF hazard~~ likelihood of failure is ~~minimized such that no further evaluation is necessary. The basis for the acceptability of this residual risk is discussed for each attribute in the subsections below.~~

~~If~~sufficiently low can be used to eliminate a CCF from further consideration. The reviewer should determine whether the application demonstrates that the use of these ~~attributes for an A1 system~~methods, alone or ~~component meet~~in any combination, meets the criteria ~~within~~in this BTP~~, then~~ to eliminate the potential CCF ~~hazard has been eliminated~~ from further consideration. ~~Thus, separate diverse means do not need to be provided, and an analysis of the plant's response for each AOO or postulated accident concurrent with a CCF of the proposed A1 system does not need to be performed for the portion of the A1 system or component that credit these attributes.~~

[22] See IEEE Std 603-1991.

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

The following sections discuss each method.

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

**Formatted:** Heading 6, Indent: Hanging: 0.5", No bullets or numbering

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

The reviewer should determine whether the proposed system contains sufficient diversity to perform the safety function, including diversity within each safety division or among redundant safety divisions of ~~an A1 system to perform the safety function, then the CCF hazard can be eliminated from further consideration.~~ 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 the reviewer can use to determine whether the system includes adequate diversity. Also, NUREG/CR-7007 identifies and develops a baseline set of diversity criteria that may characterize appropriate diversity strategies for mitigating CCF vulnerabilities. However, the quantification methodology described in NUREG/CR-7007 should not be used as the sole basis for justifying adequate diversity.

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

Acceptance Criteria

~~It should be noted that because each redundant safety-related division is credited for compliance with the single-failure criterion and is now additionally credited to prevent the CCF hazard, the allowable time that a division can be bypassed as specified in the technical specification may be more restrictive than if the redundancy is solely credited for meeting the single-failure criterion. The consistency of proposed changes and technical specifications should be addressed in the application.~~

~~Acceptance Criteria~~

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

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

b. ~~An analysis demonstrates that adequate diversity has been achieved~~Diversity between the ~~diverse~~different portions of the ~~A1~~ system or component ~~in accordance with~~ is sufficient to account for potential spurious operation.

~~b.~~c. The different portions of the ~~guidance of NUREG/CR-6303~~system or component are sufficiently diverse to perform the safety function without relying on the performance of common components, and ~~NUREG/CR-7007~~the SSCs and software of the different portions are not vulnerable to the same CCFs.

~~c.~~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~~, whose failure could affect both or all portions. ~~The~~Also, the diverse portions of the ~~A1~~ system or component do not share engineering or maintenance tools ~~that~~whose failure could affect both or all portions.

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

~~e.~~f. Periodic surveillance criteria are used to verify the ~~continued operability~~continuing functionality of each diverse ~~design~~portion.

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

~~3.1.2.~~ 3.1.2 Use of Testing to Eliminate Potential Common~~-~~Cause Failure ~~Hazard~~ from

Formatted: Indent: Left: 0"

Formatted: Indent: Left: 0"

Formatted: Indent: Left: 0"

Formatted: Normal

Formatted: Heading 6, Indent: Hanging: 0.5", No bullets or numbering, Don't keep with next

Further Consideration

~~When considering~~ CCF ~~hazards~~ vulnerabilities in DI&C systems or components~~, there are~~ have two general ~~areas of concern: (1) CCF hazards as a result of~~ causes: (1) errors introduced by the system hardware or software ~~requirements~~design, and (2) ~~CCF hazards as a result of~~ errors or defects introduced during the ~~design~~development and ~~implementation~~integration of the software, hardware, or software-based logic. ~~A~~ When designing an I&C system, the applicant might use a robust (high-quality) development process ~~can be credited to address~~, in conjunction with thorough system analysis (e.g., failure modes and effects analysis, system theoretic process analysis), to correct many potential design errors in the ~~system or component~~ requirements or specifications for both analog and digital equipment. However, ~~the~~ even a high-quality ~~of the~~ development process cannot completely eliminate ~~potential~~ latent design defects introduced during the design and ~~implementation~~integration process. ~~Testing~~

Thorough testing can help to identify latent design defects ~~that could lead to a CCF hazard~~ in DI&C systems, provided the design~~, fabrication, and implementation of software or software-based logic~~ is simple enough to allow such testing. Testing can be used to ~~both identify~~uncover latent design defects for correction in the design~~, fabrication, and implementation~~ process and to demonstrate that any ~~potential~~identified latent design defects have been corrected. The reviewer should determine whether testing of the proposed DI&C system or component shows that all latent design defects have been identified and corrected, so that the system or component will function as specified under the anticipated operational conditions. If so, the CCF can be eliminated from further consideration.

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

Acceptance Criteria

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

~~The set of test cases applicable to systems with a large number of inputs or with even a small amount of memory can become impracticably large. The testing approach provided below is intended for application to devices and components that are simple enough for such testing to be practical. For this testing to effectively represent the operational conditions expected for the component under test, this testing should be performed under anticipated operational conditions of the proposed A1 component. To credit testing as a means of demonstrating that potential design, fabrication, and implementation errors have been identified and corrected such that the device and component will function as specified under the anticipated operational conditions,~~

Formatted: Widow/Orphan control

Formatted: No underline

Formatted: No widow/orphan control, Don't keep with next

the application should demonstrate that any credited testing includes the following:

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

If the acceptance criteria below are met, the reviewer should conclude

b. If the output of a device or component depends upon timing of the input or timing of internal state changes, then the testing should include all possible timing sequences.

c. If the device or component includes any kind of memory, such that the response to the current set of inputs is dependent upon some past condition, then either all possible past condition sequences should be included in the testing or the past condition sequences should be shown through analysis to not affect the device output.

d. Any logic or circuits that are not used under any operational condition can be excluded from the test cases if it is demonstrated that the unused logic or circuitry cannot interfere with the proper operation of the device regardless of (1) any possible malfunction or failure within the device, (2) any condition external to the device, or (3) any aspect of the operation of any other logic or circuits included in the device.

Other testing methods may be acceptable and should be reviewed on a case-by-case basis. The application should provide the technical basis for using other testing methods and for how these methods are acceptable.

Acceptance Criteria

The reviewer should reach a conclusion that the application provides adequatesufficient information on the test results and testing methodology for a device or component such that a CCF hazard can be eliminated from further consideration, if the application demonstrates the following acceptance criteria are met:

a. All possible combinations of inputs have been tested as described above and the outputs have been verified to show that the output is correct for each set of inputs.

b. If the device or component depends on the timing of inputs or the timing of internal state changes, all possible timing sequences have been tested and the outputs have been verified to show that the output is correct for each set of inputs.

c. If the device or component includes any kind of memory, such that the response to the current set of inputs depends upon some past condition, then all possible past conditions have been included in the testing or have been shown through analysis to not impact the device output.

d. Any application that excludes from the test cases logic or circuits of devices or components, because they are not used under any operational condition, has demonstrated that the logic or circuits excluded do not interfere with the proper operation

Formatted: Normal

~~of the device regardless of (1) any possible malfunction or failure within the device, (2) any condition external to the device, or (3) any aspect of the operation of any other logic or circuits included in the device.~~

~~3.1.3. Use of Defensive Measures to Eliminate Common-Cause Failure Hazard from Further Consideration~~

~~Defensive measures may be used to prevent, limit, or mitigate the effects of a CCF hazard. If the application credits the use of such defensive measures to~~ to eliminate a potential CCF ~~hazard~~ from further consideration~~, the application should include the following.~~ The acceptance criteria are as follows:

Formatted: Widow/Orphan control, Keep with next

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

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

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

c. Testing results account for potential spurious operations.

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

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

an application is approved for the use described in the D3 assessment.

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

Acceptance Criteria

~~a. an identification of the vulnerabilities or hazards for which the defensive measures are being applied~~

~~b. a description of the defensive measures being credited to address the identified vulnerabilities or hazards~~

~~c. a description of~~ ~~how the CCF hazard will be prevented, limited, or mitigated by the proposed defensive measures~~

~~d. the technical basis that describes why the selected defensive measures are acceptable to address the identified vulnerabilities such that the effects of a CCF hazard are limited, mitigated, or prevented, including an analysis of how the effectiveness of the measures credited can be demonstrated~~

~~e. an assessment of any residual risks from CCF hazards~~

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

~~Acceptance Criteria~~

~~The~~ reviewer should ~~reach a conclusion~~conclude that the application provides sufficient information on the credited ~~defensive measures to eliminate a CCF hazard from further consideration~~alternative methods if ~~the application~~it includes the ~~documented~~following:

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

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

c. the supporting technical basis and acceptance criteria to demonstrate that these ~~defensive measures~~alternative methods are ~~based on an~~ NRC-approved ~~methodology. If~~

Formatted: Indent: Left: 0"

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

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

As stated above, if the application~~,~~ credits alternative methods not previously approved by the NRC, the reviewer should determine their adequacy on a case-by-case basis.

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

Formatted: Widow/Orphan control

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

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

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

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

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

Acceptance Criteria

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

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

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

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

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

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

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

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

An application that credits any of the diverse means described in Sections B.3.2.1 ~~through~~ B.3.2.3 ~~are~~of this BTP is considered ~~acceptable~~ to ~~address Position~~have acceptably addressed point 3 of the ~~SRM~~NRC position on ~~SECY-93-087, Item 18.~~D3. These diverse means include ~~crediting~~ existing systems, ~~crediting~~ manual operator ~~action~~actions, or ~~crediting a~~new diverse ~~system. The application should demonstrate the following:~~systems.

Formatted: No underline, Strikethrough

Formatted: Indent: Left: 0"

Formatted: List Paragraph, Indent: Left: 0", Hanging: 0.5", Numbered + Level: 1 + Numbering Style: a, b, c, … + Start at: 1 + Alignment: Left + Aligned at: 0.75" + Indent at: 1"

Formatted: Heading 5, Indent: Hanging: 0.5", Outline numbered + Level: 2 + Numbering Style: 1, 2, 3, … + Start at: 2 + Alignment: Left + Aligned at: 0.25" + Indent at: 0.5"

Formatted: No widow/orphan control, Don't keep with next

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

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

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

1. whether the safety function is needed,

2. whether the A1 system did not perform the safety function, and

3. whether the automated diverse means or manual operator action is successful in performing the design functions necessary to mitigate the CCF hazard.

3.2.1. 3.2.1 Crediting Existing Systems

Formatted: Heading 6, Indent: Hanging: 0.5", No bullets or numbering

An existing highly reliable I&C system can be used as a diverse means to provideaccomplish the same or a different function credited in the D3 assessment.— or to mitigate spurious operations resulting from CCF. The analysis in the LAR of the function performed by this existing I&C system should result in plant show that the consequences that do not exceed the limits prescribedof the CCF meet the acceptance criteria defined in the FSAR or the LAR for each AOO or postulated accident in the safety analysis report. An analysis should be performed to demonstratethe limiting events applicable to the proposed system or component. If an existing system is credited, then the reviewer should verify that the existing plant system to applicant performed an analysis demonstrating that the credited system and the proposed system are not both vulnerable to the same CCF.

Formatted: Widow/Orphan control

The reviewer should verify that the applicant considered how the existing system is credited in the facility's licensing basis and described in the existing system's documentation (FSAR, detailed design documents, etc.). Among other things, the reviewer should consider whether the applicant has appropriately accounted for any unique system design attributes and requirements and potential interconnectivities to other systems. The reviewer should pay particular attention to whether there may be interconnectivities the LAR has not accounted for that may result in the existing system being subject to the same CCF as the proposed DI&C system or component. The reviewer should verify that the application has identified all the features of the existing system that are relevant to demonstrating diversity. In addition, if crediting an existing system could affect the facility's existing licensing basis, then the reviewer should verify that the LAR addresses how the existing system functions would be credited and the digital design used for the proposed A1 system are not subject to the same postulated CCF. Section 2.6 of NUREG/CR-6303 identifies six diversity attributes and 25 related diversity criteria that can be used to support this qualitative analysis. NUREG/CR-7007 identifies and develops justified in a baseline set of diversity criteria that may constitute appropriate mitigating diversity strategies to address vulnerabilities to CCF hazards. revised licensing basis.

The credited existing system may be a system that isan NSR providedsystem, as long as it is of

sufficient quality and can reliably perform the credited functions under the associated event conditions. ~~For existing systems that are~~ If the applicant credits NSR~~, the quality of~~ systems that are in continuous use (e.g., the normal reactor coolant system inventory control system or the normal steam generator level control system), these systems ~~should be similar to systems required by the ATWS rule~~need not meet augmented quality standards. However, if the applicant credits NSR systems that are not in continuous use (i.e., ~~10 CFR 50.62), as described in the enclosure to Generic Letter 85-06.~~that are normally in standby mode), then the reviewer should verify that the applicant demonstrated that the system will reliably perform its intended function. For example, the applicant may credit the plant ATWS ~~design capabilities may be credited~~system as a diverse means of achieving reactor shutdown, provided that the ATWS system ~~design to be credited~~ is capable of responding to the same analyzed events as the proposed ~~A1~~DI&C system. ~~The~~In this case, the reviewer should consider whether the D3 analysis demonstrates that the ATWS system ~~to be credited should~~ (1) ~~be diverse from~~is not vulnerable to the same CCF as the equipment performing the reactor trip function within the proposed DI&C system, (2) ~~has been demonstrated to be highly reliable and~~is of sufficient quality and is capable of functioning under the event conditions expected, and (3) ~~be~~is responsive to the AOO or ~~postulated accident~~PA sequences ~~using independent sensors and actuators as the proposed DI&C system~~.

~~Acceptance Criteria~~

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

Acceptance Criteria

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

a. ~~The~~If NSR equipment ~~to be credited~~ is ~~highly reliable,~~ used in the diverse system, the equipment is of sufficient quality~~, and is expected to be available~~ to perform the necessary function(s) during the associated event conditions. Sufficient quality can be

Formatted: Tab stops: 0.63", Left

Formatted: No underline

Formatted: Indent: Left: 0"

achieved, for example, through application of the alternative treatment requirements developed for implementation of 10 CFR 50.69 or the ATWS quality assurance guidance set forth in GL 85-06.

b. ~~The equipment to be credited is~~Sufficient diversity exists between the diverse system and the proposed system, so that they are not subject to the same postulated CCF ~~as the proposed DI&C system~~.

c. The equipment to be credited ~~(1)~~ has ~~the~~functional capabilities ~~of sensing and respondingsufficient~~ to ~~the same plant conditions as the affected system if performing the same safety function, or (2) is capable of sensing and responding to alternative plant conditions if performing a different function. For both these options, the application should show that the capabilities for sensing and responding~~ maintain ~~plant safety by verifying plant conditions stay~~ the plant within the acceptance criteria ~~specified for each AOO or postulated accidentdefined~~ in the ~~safety analysis report~~FSAR or the LAR for the limiting events applicable to the proposed DI&C system or component.

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

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

~~3.2.2.~~ 3.2.2 Crediting Manual Operator Action

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

The reviewer should consider whether the equipment necessary to perform ~~such action~~these actions, including the supporting indications~~, should be diverse and independent from~~ and controls, is diverse from (i.e., not vulnerable to the same sources of CCF as) the equipment performing the same function within the safety-related I&C system ~~disabled by a postulated~~

**Formatted:** Indent: Left: 0"

**Formatted:** Indent: Left: 0"

**Formatted:** List Paragraph

**Formatted:** Heading 6, Indent: Hanging: 0.5", No bullets or numbering

**Formatted:** Widow/Orphan control

CCF.  If the equipment used to perform the credited manual operator action is NSR, then the applicationapplicant should include information to demonstrate that the equipment used is highly reliable and of sufficientadequate quality. This equipment should be similar in quality to that required—for example, by applying the ATWS rule (i.e., alternative treatment requirements in 10 CFR 50.62), as described in the enclosure to Generic Letter69 or the ATWS quality assurance guidance in GL 85-06.  Functional characteristics (e.g., range, accuracy, time response) should be sufficient to provide operators with the information needed to place and maintain a plant in a safe shutdown condition.  A CCF hazard that affects normal displays or controls should not prevent the operator from manually performing the safety functions.

The application should contain an HFE analysis in accordance with the guidance of SRP Chapter 18, to demonstrate that plant conditions can be maintained within specified acceptance criteria for the particular AOO or postulated accident.  The credited manual operator action and the equipment necessary to perform the action should be identified.  If If the applicant proposed the use of equipment outside of the MCR is used to perform the credited manual operator action, then the reliability, availability, and accessibility of the reviewer should consider whether this equipment is vulnerable to the same CCF as the safety system and whether the applicant demonstrated that the equipment will be reliable, available, and accessible under the postulated event conditions should be demonstrated.  The reviewer may use the HFE principles and criteria should be applied to theidentified in SRP Chapter 18 to evaluate the applicant's selection and design of the displays and controls.  Human performance requirements should be described and related to the plant safety criteria.  Recognized human factors standards and design techniques should be employed to support the described human-performance requirementsIn addition, the reviewer may use the guidance in NUREG-1764, Revision 1, to perform a risk-informed evaluation of the application.

Protective Actions Initiated Solely by Manual Actions

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

Acceptance Criteria

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

a. The manual operator action can be performed within an acceptable time frame as specified in SRP Chapter 18.  The difference between the time available to perform the operator action, as determined by the thermal-hydraulic analysis, and the time necessary to perform it, as determined by the HFE analysis, is a measure of the safety margin.  As this margin decreases, the uncertainty in the estimate of the difference between these times should be appropriately considered.  This uncertainty could reduce

Formatted: Widow/Orphan control

Formatted: Tab stops:  0.63", Left

Formatted: No underline

the level of assurance and potentially invalidate a conclusion that operators can reliably perform the action within the time available. For complex situations and for manual operator action with limited margin between time available and time necessary, a more focused staff review will be performed.

b. The equipment used to support manual operator action is diverse, reliable, of sufficient quality, available, and accessible during the associated event conditions.

c. The indications and controls needed to support the manual operator action has the functional characteristics necessary to maintain the plant within the accepted limits.

d. The HFE analysis demonstrates the acceptance criteria provided in SRP Chapter 18, have been met.

3.2.3. Crediting a Diverse System

A diverse system (e.g., diverse actuation system), including automated or manual functions, or both, can be used as a diverse means to provide the same or a different function credited in the D3 assessment. If such a system is credited as a diverse means to address CCF hazards, the application should demonstrate that (1) the functions performed by this diverse means are adequate to maintain plant conditions within specified acceptance criteria for the associated DBE and (2) sufficient diversity exists between this diverse system and the A1 system such that a postulated CCF cannot disable both systems. An analysis should be performed to demonstrate that the diverse means to be credited and the digital design used for the proposed A1 system are not subject to the same CCF hazard. Section 2.6 of NUREG/CR-6303 identifies six diversity attributes and 25 related diversity criteria that can be used to support this qualitative analysis.

The diverse means may be performed by a system that is NSR, if the system is of sufficient quality to perform the necessary function(s) under the associated event conditions. The diverse means should be similar in quality to systems required by the ATWS rule (i.e., 10 CFR 50.62), as described in the enclosure to Generic Letter 85-06.

Prioritization between A1 systems and the diverse system should address the following to ensure the credited safety function can be accomplished by either system:

a. Commands that direct a component to a safe state should always have the highest priority and override other commands. The term "safe state" refers to a predetermined design state of least critical consequence.

b. For those components with multiple safe states, in which each safe state is defined by the plant conditions, priority should be assigned based upon considerations relating to plant system design to minimize consequence to plant safety.

c. The basis behind the proposed priority ranking should be explained in detail.

Formatted: Indent: First line: 0"

Formatted: Underline

Formatted: Normal, No bullets or numbering, Tab stops: 0.63", Left

Formatted: Indent: First line: 0", Tab stops: 0.63", Left

d. The priority function should be shown to apply the commands correctly in order of their priority rankings and should meet all other applicable guidance.

Acceptance Criteria

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

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

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

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

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

e. If equipment that is NSR is used in the diverse system, the equipment is highly reliable and of sufficient quality to perform the necessary function(s) during the associated event conditions.

3.3. Consequences of the CCF Hazard Are Acceptable

For each event analyzed in accident analysis, either best estimate methods (i.e., using realistic assumptions to analyze the plant response to DBEs) or conservative methods (i.e., design basis analysis) may be used to perform the D3 assessment. This assessment should show that consequences of CCF hazards of an A1 or portions of an A1 system are acceptable per the acceptance criteria below.

Acceptance Criteria

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

a. For each AOO in the design basis occurring in conjunction with the CCF hazard, the plant response calculated using realistic or conservative assumptions does not result in radiation release exceeding 10 percent of the applicable siting dose guideline values or

Formatted: No underline
Formatted: No widow/orphan control, Don't keep with next
Formatted: List Paragraph, Indent: First line: 0"
Formatted: No underline
Formatted: Tab stops: Not at 0.63"
Formatted: No widow/orphan control, Don't keep with next

violation of the integrity of the primary coolant pressure boundary.

b. For each postulated accident in the design basis occurring in conjunction with each single postulated CCF, the plant response calculated using realistic or conservative assumptions does not result in radiation release exceeding the applicable siting dose guideline values, violation of the integrity of the primary coolant pressure boundary, or violation of the integrity of the containment (i.e., exceeding coolant system or containment design limits).

4. Qualitative Assessment

RIS 2002-22, Supplement 1, describes a methodology that the NRC staff finds acceptable to assess the likelihood of failure of a proposed modification of an SSC with digital technology, referred to as a qualitative assessment. The qualitative assessment described in RIS 2002-22, Supplement 1, is intended for modifications to SSCs of low safety significance (i.e., A2 and B1) and not for SSCs of high safety significance (i.e., A1 systems).

The qualitative assessment considers three factors that, when taken in the aggregate, can be used to demonstrate that a proposed digital modification to an SSC will exhibit a low likelihood of failure (e.g., low likelihood of CCF) such that likelihood of failure of the proposed DI&C system is consistent with the assumptions in the SAR. These three factors include:

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

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

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

Consideration of these factors, as well as supporting failure analysis information as described in RIS 2002-22, Supplement 1, is an acceptable method to address CCF hazards in A2, B1, and applicable B2 systems. The application should include a qualitative assessment that documents (1) how these three factors have been used to reduce the likelihood of CCF hazards to eliminate it from further consideration, and (2) the supporting failure analysis.

Acceptance Criteria

As described in RIS 2002-22, Supplement 1, the acceptance criteria used to determine whether an SSC has a low likelihood of failure such that current licensing assumptions continue to be met are referred to as "sufficiently low." The concept of "sufficiently low" was developed to address the likelihood of a CCF hazard due to latent digital defects of a system or component modified with digital technology. The "sufficiently low" definition incorporates consideration of failure likelihood of a proposed SSC to failures documented in the SAR. This approach can also be used for a new reactor design.

The reviewer should reach a conclusion that the application has addressed a CCF hazard in A2, B1, or applicable B2 systems if the application provides a qualitative assessment demonstrating

Formatted: Widow/Orphan control

Formatted: No underline, Strikethrough

Formatted: Right: 0.5"

Formatted: Not Strikethrough

Formatted: List Paragraph

~~the likelihood of the CCF hazard is sufficiently low based on any of the following criteria :~~

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

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

~~c. The applicable operating experience~~ regarding the DI&C system or component ~~collectively supports a conclusion that the DI&C system or component will operate with high~~ reliability ~~for the intended application. Operating experience in most cases can serve to compensate for weakness in addressing the other two criteria~~of the proposed manual actions.

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

~~5. Spurious Operation Assessment~~

~~5.1. Operating Reactors Not Required To Address IEEE Std 603-1991~~

~~For proposed DI&C modifications in plants not licensed under IEEE Std 603-1991, the application should include an assessment demonstrating that the spurious operations assumed in the accident analysis are not invalidated by the proposed modification to the DI&C system.~~

Acceptance Criteria

~~The~~ If the following acceptance criteria are met, the reviewer should ~~reach a conclusion~~conclude that the proposed manual operator action is acceptable:

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

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

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

**Formatted:** Indent: Left: 0"

**Formatted:** Normal, No bullets or numbering

**Formatted:** Don't keep with next

**Formatted:** Indent: First line: 0"

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

3.2.3 Crediting a New Diverse System

The applicant may propose a new diverse system (e.g., a diverse actuation system) as a diverse means of accomplishing the same or a different function credited in the D3 assessment or of mitigating spurious operation ~~assessment if the~~ due to CCF. In this case, the reviewer should determine whether the application demonstrates that (1) the functions performed by this diverse means suffice to maintain plant conditions within specified acceptance criteria for the associated DBE, and (2) sufficient diversity exists between the new system and the proposed DI&C system so that they are not vulnerable to the same postulated CCF. The reviewer should determine whether the diverse means credited and the digital design of the proposed system are vulnerable to the same CCF. Section 2.6 of NUREG/CR-6303 identifies six diversity attributes and 25 related diversity criteria that the reviewer can use to determine whether the new diverse system is adequate to mitigate the CCF.

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

Prioritization

If a new diverse system is implemented, the reviewer should verify that the signals to actuate components coming from the different systems are appropriately prioritized to maintain the overall defense-in-depth strategy. If the proposed DI&C system and the new diverse system share resources (e.g., priority modules), the reviewer should consider whether the proposed DI&C system has priority in the use of shared resources in regard to its safety and protection functions, so that safety and protection functions are always carried out first. DI&C-ISG-04 provides guidance on prioritization of control and protection systems sharing components. (In some cases, certain components may have more than one safe state; the reviewer should consider whether the priority scheme describes all safe states.)

Acceptance Criteria

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

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

Formatted: Underline

Formatted: Underline

Formatted: Normal, Space After: 0 pt, No bullets or numbering, Keep with next

Formatted: Widow/Orphan control, Keep with next

assurance guidance set forth in GL 85-06.

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

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

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

3.3 Consequences of a Common-Cause Failure May Be Acceptable

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

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

Acceptance Criteria

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

a. For ~~the~~ those postulated spurious operations that have not been fully mitigated or eliminated from further consideration, the consequences of spurious operation of safety-related or NSR components ~~or components that~~ are ~~NSR assumed~~bounded by the acceptance criteria defined in the ~~accident analysis have not been invalidated by the proposed modification of~~ FSAR or the ~~DI&C system or component.~~LAR.

~~5.2. IEEE Std 603-1991 Applies~~

~~Pursuant to the incorporation by reference in 10 CFR 50.55a, IEEE Std 603-1991, Clauses 4.8 and 5.6.3, require that safety-related systems be designed to prevent conditions that can lead to performance degradations of the safety-related system. This includes conditions such as~~

Formatted: List Paragraph, Indent: First line: 0"

Formatted: No underline

Formatted: Normal, No bullets or numbering, Tab stops: 0.63", Left

Formatted: Indent: First line: 0", Tab stops: 0.63", Left

Formatted: Underline

Formatted: Tab stops: 0.63", Left

Formatted: Widow/Orphan control, Keep with next

Formatted: List Paragraph, Indent: Left: 0", Hanging: 0.5", Outline numbered + Level: 5 + Numbering Style: a, b, c, … + Start at: 1 + Alignment: Left + Aligned at: 2.25" + Indent at: 2.5", Don't keep with next

Formatted: List Paragraph, Indent: Hanging: 0.5", Don't keep with next

~~failures or consequential actions by systems that are NSR that could lead to spurious operation of both safety-related components and components that are NSR. For DI&C systems in plants that have IEEE Std 603-1991 as part of their licensing basis or for applications for CPs, OLs, SDAs, DCs, COLs, or MLs, the potential for spurious operation resulting from a CCF hazard of the DI&C system should be assessed using the following considerations:~~

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

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

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

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

b. ~~The consequences of the initiating event created by the spurious operation of safety-related components or components that are NSR are acceptable per the acceptance criteria within Section B.3.3.~~ For each AOO in the design basis that occurs concurrently with the CCF, the plant response, calculated using realistic or conservative assumptions, does not result in radiation release exceeding 10 percent of the applicable siting dose guideline values, or in violation of the integrity of the primary coolant pressure boundary.

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

~~3.~~ 4.

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

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

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

**Formatted:** Normal, Space After: 0 pt, No bullets or numbering, Keep with next

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

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

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

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

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

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

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

Formatted: Normal, Space After: 0 pt, No bullets or numbering, Keep with next

Acceptance Criteria

Formatted: Widow/Orphan control, Keep with next

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

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

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

c. Any automatic functions or manual operator action credited to mitigate the conditions caused by potential spurious operation of safety-related components or components that are NSR meet the acceptance criteria within Section B.3.2.

d. For those CCF hazards that have not been shown to be mitigated or prevented, consequences resulting from spurious operation of safety-related components or components that are NSR are bounded by the events analyzed in the accident analysis.

6. Manual System -Level Actuation and Indications to Address Position 4 of the SRM on SECY-93-087, Item 18.Point 4

Formatted: Heading 4, No bullets or numbering, Keep with next

Formatted: Widow/Orphan control, Keep with next

Displays and Point 4 of the NRC's position on D3 states that the applicant shall provide a set of displays and controls in the MCR for manual system-level actuation of critical safety functions

and monitoring of parameters that support the safety functions. Section B.1.2 defines critical safety functions. RG 1.62 outlines important design criteria for I&C equipment used by plant operators for manual initiation of protective actions.

The reviewer should consider whether displays and manual controls provided ~~for compliance with Position 4 of the SRM on SECY-093-87, Item 18 should be sufficient both to monitor the plant state and~~ to meet point 4 are not vulnerable to ~~enable control room operators to actuate critical safety functions. For~~ the same CCF as the proposed DI&C system ~~modifications to operating plants, retention of existing~~. For example, the point at which the credited manual controls are connected to the safety equipment should be downstream of the equipment that can be adversely affected by a CCF. The reviewer should confirm that the applicant does not credit the same digital platform or analog ~~displays and controls in the MCR could satisfy Position 4. However, if existing~~technology for point 3 (e.g., to mitigate DBEs). Point 4 specifies that the MCR displays and controls ~~are digital, or the same platform is used both for mitigating the DBE~~shall be independent and ~~to provide signals to these~~diverse from the digital platform or analog ~~displays~~technology identified for points 1 and ~~controls, retaining existing analog~~ 3.

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

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

a. ~~The displays and~~The reviewer should determine whether controls ~~should be sufficient for the operator to monitor and control the following critical safety functions: reactivity, core heat removal, reactor coolant inventory, containment isolation, and containment integrity.~~

b. ~~The indication and manual controls to actuate~~outside the MCR are exclusively used for long-term management of these critical safety functions ~~should be at the~~, after completion of system ~~–~~level or division ~~level and located within the MCR.~~

c. ~~Equipment that is NSR may be used for these manual controls and indications, provided that the equipment is reliable and of sufficient quality. This equipment should be similar in quality to that required by the ATWS rule (i.e., 10 CFR 50.62), as described in the enclosure to Generic Letter 85-06.~~

d. ~~The displays and controls should be diverse from the safety-related DI&C systems that are vulnerable to a CCF hazard such that these display and controls are not affected by potential CCFs that could disable the safety-related DI&C systems.~~

~~Once system- or division-~~level manual actuation from the MCR using the ~~Position~~point 4 displays and controls ~~has been completed,~~. The reviewer should also determine whether

controls outside the MCR ~~for long-term management of these critical safety functions may be used when~~are supported by suitable HFE analysis and site-specific procedures or instructions.

~~Acceptance Criteria~~

~~The~~
Acceptance Criteria

If the following acceptance criteria are met, the reviewer should ~~reach a conclusion~~conclude that the manual controls and supporting ~~indications conform~~displays meet point 4:

a. proposed manual actions credited to ~~Position 4~~accomplish safety functions that would otherwise have been accomplished by automatic safety systems are both feasible and reliable, as demonstrated through an HFE analysis, such as the one described in SRP Chapter 18. Section B.3.2.2 of ~~the SRM on SECY-93-087, Item 18, if the~~ this BTP presents the acceptance criteria for manual actions.

The application ~~demonstrates the following acceptance criteria have been met:~~

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

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

~~b.~~d. The manual controls for ~~these~~ critical safety functions are at the system or division level and are located within the MCR. ~~Since single failures concurrent with a CCF do not need to be postulated and normal alignment of equipment is assumed, the capability for manual actuation of a single division is sufficient.~~ For plants licensed to allow one division to be continuously out of service, the diverse manual actuation applies to at least one division that is in service.

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

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



Formatted: Underline
Formatted: Tab stops: 0.63", Left
Formatted: Widow/Orphan control, Keep with next
Formatted: Indent: Left: 0"
Formatted: List Paragraph, Indent: First line: 0"
Formatted: Indent: Left: 0"

## ~~7.~~5. Information ~~To Be Reviewed~~for Interdisciplinary NRC Staff Review

~~The information to be reviewed should be commensurate with safety significance of the DI&C system under evaluation. The following information should be reviewed:~~

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

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

~~b. For an A1 system,~~ the results of ~~the~~any D3 assessment, ~~specifically, the following:~~

~~1.~~b. ~~Identification of any credited design attribute or defensive measure to eliminate CCF hazards from further~~ including consideration ~~and a demonstration that these attributes or measures are effective. Identification of any remaining vulnerabilities to CCF hazards.~~of spurious operations, and specifically the following:

– ~~For CCF hazards that have not been eliminated~~any means used to eliminate potential CCFs from further consideration, ~~identification of~~ any information demonstrating that these means are effective, and any remaining CCF vulnerabilities (residual risks)

~~2.~~ any diverse means provided by the applicant to accomplish the same or a different function than the safety function disabled by a postulated CCF. ~~If~~ for any CCFs not eliminated using design attributes (if any diverse means ~~are~~is credited to mitigate the ~~CCF hazard, the NRC staff should review~~ potential CCF, the information provided to demonstrate the its effectiveness of the diverse means, including ~~any~~ assessment from the results of HFE analysis associated with of any manual operator ~~action~~actions if used as a diverse means.~~–~~)

~~3.~~ ~~For CCF hazards~~the results of any consequence analysis that ~~have~~the applicant has performed for CCFs not ~~been~~ eliminated from further consideration ~~or~~, mitigated using diverse means, ~~identification of any~~are verified as being acceptable, with such an analysis ~~performed to demonstrate~~demonstrating that the consequences of ~~a~~the CCF ~~hazard~~ are within acceptable limits for each AOO and ~~postulated accident. If any consequence analysis has been performed, the NRC staff should review the results of this analysis.~~ PA

~~c. For A2 and B1~~ for systems~~, the results of the qualitative assessment of these systems, specifically, the following:~~



**Formatted:** Heading 4, Indent: Hanging: 0.5", Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 5 + Alignment: Left + Aligned at: 0.25" + Indent at: 0.5", Don't keep with next

**Formatted:** Indent: Left: 0", Hanging: 0.5"

**Formatted:** Indent: Left: 0.5", Hanging: 0.5", Outline numbered + Level: 2 + Numbering Style: Bullet + Aligned at: 0.25" + Indent at: 0.55", Widow/Orphan control

**Formatted:** Indent: Left: 0.5", Hanging: 0.5"

**Formatted:** Indent: Left: 0.5", Hanging: 0.5", Outline numbered + Level: 2 + Numbering Style: Bullet + Aligned at: 0.25" + Indent at: 0.55", Widow/Orphan control

1. ~~Information supporting the use of design attributes and features to reduce the likelihood of a CCF hazard such~~ that ~~it is sufficiently low.~~

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

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

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

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

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

2. ~~Vulnerabilities to potential spurious operations due to a CCF hazard in an A2 or B1 system have been addressed through use of a combination of the three factors described in Section B.~~for manual system-level actuation and indications to address point 4~~; or~~

3. ~~The consequence of a potential spurious operation due to a CCF hazard is bounded by the accident analysis;~~

d. ~~For a proposed A1 system~~, design information showing ~~that~~ the following:

~~f.~~ controls and displays~~:~~

1. ~~Have been~~ provided in the MCR to perform manual system~~-~~ or division~~-~~level actuation of critical safety functions~~;~~

2. ~~Are~~ controls and displays are independent and diverse from the ~~A1 system such~~equipment performing the same functions within the proposed DI&C system, so that they are not ~~subject~~vulnerable to the same CCF ~~hazard~~ as the ~~A1~~proposed system~~; and~~

3. ~~Have adequate~~controls and displays have sufficient quality to support the manual

**Formatted:** Indent: Left: 0.5", Hanging: 0.5", Bulleted + Level: 1 + Aligned at: 0.25" + Indent at: 0.5"

**Formatted:** Indent: Left: 0.5", Hanging: 0.5", Bulleted + Level: 1 + Aligned at: 0.25" + Indent at: 0.5"

**Formatted:** Indent: Left: 0.5", Hanging: 0.5", Bulleted + Level: 1 + Aligned at: 0.25" + Indent at: 0.5"

operator ~~action~~actions during the associated event ~~condition~~conditions, if the equipment used is NSR~~.~~

~~8. Review Procedures~~

6. ~~In reviewing the D3 assessment results in accordance with~~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~~, emphasis should be given to~~ to evaluate the applicant's D3 assessment. During this evaluation, the reviewer should consider the topics described below~~:~~.

~~8.1.~~6.1 System Representation as Blocks

**Formatted:** Heading 5, Indent: Hanging: 0.5", Outline numbered + Level: 2 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Indent at: 0.5"

~~The system being assessed is represented as a block diagram; the inner workings of the blocks are not necessarily shown. A block is~~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 ~~software and logic errors~~latent design defects, will not propagate to ~~other~~ equipment or software~~.~~ outside of the block. A block can also be a software macro~~/~~ or subroutine, such as a voting block or a proportional~~-~~integral~~-~~derivative block, that is used by multiple functional applications~~; a design or implementation defect in this type of block can result in a CCF hazard~~. Representations of ~~all application functions that utilize that~~systems or components using blocks may not show the inner workings of each block. ~~Diversity is determined at the block level.~~

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

~~8.2.~~6.2 Documentation of Assumptions

**Formatted:** Heading 5, Indent: Hanging: 0.5", Outline numbered + Level: 2 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Indent at: 0.5"

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

~~8.3. Effect of Other Blocks~~

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

~~hazard under consideration.~~

~~8.4.~~6.3 Identification of Alternate Trip or Initiation Sequences

~~The~~The reviewer should verify that the applicant's assessment includes thermal-hydraulic analyses ~~using realistic assumptions~~ of the sequence of events that would occur if the primary trip channel failed to trip the reactor or actuate ~~ESF. Coordination~~ESFs. The thermal-hydraulic analyses may use realistic or conservative (design-basis) assumptions. When evaluating these analyses, the reviewer should coordinate with the NRC staff organization responsible for the review of reactor systems ~~is necessary in reviewing these analyses~~.

~~8.5.~~6.4 Identification of Alternative Mitigation Capability

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

~~When operator action is cited as~~ If the application cites a manual operator action as a diverse means for ~~response~~responding to an event, the ~~applicant~~reviewer should ~~demonstrate~~verify that the applicant's HFE analysis ~~is adequate~~demonstrates (e.g., through the process in ~~accordance with~~ SRP Chapter 18~~. Coordination~~) that this action is both feasible and reliable. For this, the reviewer should coordinate with the organization responsible for the review of human-~~-~~system interfaces ~~for any credited diverse manual operator action should be included as part of this activity~~.

~~8.6.~~6.5 Justification for Not Correcting Specific Vulnerabilities

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

**Formatted:** Heading 5, Indent: Hanging: 0.5", Outline numbered + Level: 2 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Indent at: 0.5"

**Formatted:** Heading 5, Indent: Hanging: 0.5", Outline numbered + Level: 2 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Indent at: 0.5"

**Formatted:** Heading 5, Indent: Hanging: 0.5", Outline numbered + Level: 2 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Indent at: 0.5"

## C. REFERENCES


1. ~~Institute~~ *U.S. Code, of Federal Regulations* (CFR), "Domestic Licensing of Production and Utilization Facilities," Part 50, Chapter I, Title 10, "Energy."

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

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

~~1.~~4. Institute of Electrical ~~&~~and Electronics Engineers, ~~IEEE 100,~~ "The Authoritative Dictionary of IEEE Standards Terms," IEEE 100, Piscataway, NJ.

~~2.~~5. Institute of Electrical ~~&~~and Electronics Engineers, ~~IEEE Std 279-1968,~~ "Proposed IEEE Criteria for Nuclear Power Plant Protection Systems," IEEE Std 279-1968, Piscataway, NJ.

~~3.~~6. Institute of Electrical ~~&~~and Electronics Engineers, ~~IEEE Std 279-1971,~~ "Criteria for Protection Systems for Nuclear Power Generating Stations," IEEE Std 279-1971, Piscataway, NJ.

~~4.~~7. Institute of Electrical ~~&~~and Electronics Engineers~~, IEEE Std 379-2000~~, "IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems," IEEE Std 379-2000, Piscataway, NJ.

~~5.~~8. Institute of Electrical ~~&~~and Electronics Engineers, ~~IEEE Std 603-1991,~~ "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," IEEE Std 603-1991, Piscataway, NJ.

~~6.~~9. Institute of Electrical ~~&~~and Electronics Engineers, ~~IEEE Std 603-1991,~~ "Standard Criteria for Safety Systems for Nuclear Power Generating Stations," IEEE Std 603-1991 Correction Sheet, January 30, 1995.

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

~~7.~~11. U.S. Nuclear Regulatory Commission, "A Defense-in-Depth and Diversity Assessment of the RESAR-414 Integrated Protection System," NUREG-0493, March 1979.


Formatted: Widow/Orphan control

Formatted: Widow/Orphan control, Keep with next

Formatted: Font: Italic

Formatted: Widow/Orphan control

Formatted: Widow/Orphan control

Formatted: Widow/Orphan control

8.12. U.S. Nuclear Regulatory Commission, "Application of the Single-Failure Criterion to Safety Systems," Regulatory Guide 1.53.

13. U.S. Nuclear Regulatory Commission, "ControlCriteria for Use of Computers in Safety Systems of Nuclear Power Plants," Regulatory Guide 1.152.

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

9.15. U.S. Nuclear Regulatory Commission, "Regulatory Requirements, Acceptance Criteria, and Guidelines for Instrumentation and Control Systems Important to Safety," NUREG-0800, SRP Section 7.7.1-T.

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

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

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

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

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

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

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

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

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

11. U.S. Nuclear Regulatory Commission, "Diverse Instrumentation and Control Systems," NUREG-0800, SRP Section 7.8.

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

Formatted: Widow/Orphan control

Formatted: Widow/Orphan control

Formatted: Widow/Orphan control

Formatted: Widow/Orphan control

13. U.S. Nuclear Regulatory Commission, "Human Factors Engineering," NUREG-0800, SRP Chapter 18.

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

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

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

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

18.30. U.S. Nuclear Regulatory Commission, "Quality Assurance Guidance for ATWS Equipment That Isis Not Safety-Related," Generic Letter 85-06, April 16, 1985.

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

Formatted: Normal

Formatted: Widow/Orphan control

**Paperwork Reduction Act Statement**

~~This Standard Review Plan provides voluntary guidance for implementing the mandatory information collections in 10 CFR Parts 50 and 52 that are subject to the Paperwork Reduction Act of 1995.~~

~~(44 U.S.C. 3501 et. seq.). These information collection were approved by the Office of Management and Budget (OMB), approval numbers 3150-0011 and 3150-0151. Send comments regarding this information collection to the Information Services Branch (T6-A10M), U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001, or by e-mail to Infocollects.Resource@nrc.gov, and to the OMB reviewer at: OMB Office of Information and Regulatory Affairs (3150-0011, 3150-0151), Attn: Desk Officer for the Nuclear Regulatory Commission, 725 17th Street, NW Washington, DC 20503; e-mail: oira_submission@omb.eop.gov.~~

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~~Office of Management and Budget control number.

**BTP Section 7-19**

**Description of Changes**

**~~BTP 7-19, "~~GUIDANCE FOR EVALUATION OF DEFENSE IN DEPTH AND DIVERSITY TO ADDRESS COMMON ~~-~~CAUSE FAILURE ~~HAZARDS~~ DUE TO LATENT ~~SOFTWARE~~DESIGN DEFECTS IN DIGITAL ~~INSTRUMENTATION AND CONTROL~~SAFETY SYSTEMS~~"~~**

Formatted: Font: Bold

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

The main purpose of this update is to ~~provide clarification on~~clarify sections of the guidance that proved challenging to implement ~~based upon~~, according to feedback received by internal and external stakeholders. ~~This~~The update improves readability and ~~the~~ flow ~~of information such that it is~~to make it clear to the reader that there is an established process for analyzing potential ~~hazards caused by CCFs of~~vulnerabilities to common-cause failures resulting from latent design defects in digital technology, in particular within hardware, and software or software ~~-~~-based logic. ~~This~~The update clarifies the scope of applicability for all users ~~as well as~~and clearly ~~stating the applicability of~~ states that this guidance does not apply to the ~~10 CFR 50.59~~ change process~~.~~ in Title 10 of the *Code of Federal Regulations* 50.59, "Changes, tests and experiments." The update provides for ~~a graded approach that clarifies the technical rigor and analysis that's appropriate for SSCs~~structures, systems, and components of differing safety ~~class~~significance, so that an adequate demonstration of safety ~~for a proposed modification~~ is consistently applied. ~~This is in addition to clarifying~~ It also clarifies specific areas of guidance, such as diversity and testing ~~to eliminate further consideration~~, and adds the concepts of alternative methods, qualitative assessment, and supporting failure analysis as means of ~~CCF hazards. Lastly, the update revises the flow and structure of the BTP's guidance to improve readability so that the user clearly understands the overall process for~~ addressing ~~CCF hazards.~~common-cause failures.

**Page 1: [1] Style Definition** **Notich, Mark** **12/28/2020 1:57:00 PM**

Comment Text: Right, Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at:  0.25" + Indent at:  0.5"

**Page 1: [2] Style Definition** **Notich, Mark** **12/28/2020 1:57:00 PM**

Heading 6: Font: Arial, Not Bold, Indent: Left:  0.5", Space Before:  0 pt, After:  0 pt, Don't add space between paragraphs of the same style

**Page 1: [3] Style Definition** **Notich, Mark** **12/28/2020 1:57:00 PM**

Heading 5: Font: 11 pt, Not Bold, Not Italic, Indent: Left:  0", Hanging:  0.5", Space Before:  0 pt, After:  0 pt, Don't add space between paragraphs of the same style, Outline numbered + Level: 2 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: