



U.S. NUCLEAR REGULATORY COMMISSION

# STANDARD REVIEW PLAN

## BRANCH TECHNICAL POSITION 7-19

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

#### REVIEW RESPONSIBILITIES

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

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

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

Draft Revision 8 – May 2020

---

#### USNRC STANDARD REVIEW PLAN

This Standard Review Plan, NUREG-0800, has been prepared to establish criteria that the U.S. Nuclear Regulatory Commission 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 is not a substitute for the 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 evaluate how the proposed alternatives to the SRP acceptance criteria provide an acceptable method of complying with the NRC regulations.

The standard review plan sections are numbered in accordance with corresponding sections in Regulatory Guide 1.70, "Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants (LWR Edition)." Not all sections of Regulatory Guide 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 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.

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 email to [DISTRIBUTION@nrc.gov](mailto: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.

---

Power Plants: LWR Edition,” (SRP), Section 7.1-T, “Regulatory Requirements, Acceptance Criteria, and Guidelines for Instrumentation and Control Systems Important to Safety” (Table 7-1). References to industry standards incorporated by reference into regulations (Institute of Electrical and Electronics Engineers (IEEE) Standard (Std) 279-1968, IEEE Std 279-1971, and IEEE Std 603-1991) and industry standards that are not endorsed by the agency do include the associated year in this BTP. See Table 7-1 to ensure that the appropriate RGs and endorsed industry standards are used for the review.

## **A. BACKGROUND**

While digital technology offers significant operational and maintenance benefits for safety systems of nuclear power plants (NPPs), the development of such systems needs to address vulnerability to potential common-cause failures (CCFs). The ability to integrate design functions using digital instrumentation and control (DI&C) technology makes the identification and evaluation of potential consequences of a postulated CCF more challenging. The potential adverse consequences of integrating design functions must be considered when design functions of different systems are either directly incorporated into the same DI&C system (i.e., software platform) or indirectly when the DI&C system incorporates shared resources. Shared resources include the implementation of bidirectional digital communications, networks, common controllers, power supplies, or multifunction display and control stations. Shared resources and interconnectivity introduced by proposed DI&C systems have the potential to reduce the redundancy, diversity, separation, or independence of systems described in the facility’s safety analysis report (SAR).

DI&C systems are composed of both hardware components and logic elements (e.g., software). Hardware components in DI&C systems are susceptible to failures and faults, similar to those considered for analog systems. Regarding the logic portion, DI&C systems or components can also be vulnerable to a CCF due to latent defects in hardware, software, or software-based logic. Events or plant conditions can trigger latent defects in hardware, software, or system components within redundant portions (e.g., safety divisions) of a system designed to perform safety functions, and thus lead to a systematic fault. The effects of a CCF can include the potential loss of the capability to perform a safety function, or initiation of a plant transient not previously analyzed. The CCF could arise as a systematic fault during anticipated operational occurrences (AOOs), postulated accidents (PAs), or normal operations. This BTP provides the U.S. Nuclear Regulatory Commission (NRC) staff with guidance for evaluating applicant or licensee analyses of proposed DI&C safety systems and their vulnerabilities to CCFs resulting from systematic faults caused by latent defects in the software, hardware, or software-based logic.

A CCF of a DI&C system or component can also initiate the operation of a safety function or other design functions without a valid demand, or can result in erroneous (i.e., spurious) system actions. These conditions are typically referred to as “spurious operations,” or “spurious actuation.” (This BTP, uses the term “spurious operations.”) This BTP also provides the staff with guidance for evaluating applicant or licensee evaluations of a proposed modification to

withstand or cope with CCFs resulting from spurious operations originating from key plant control systems.

### Types of Failure Considerations

The possible outcomes and consequences of CCFs in DI&C systems should be evaluated to ensure that potential CCFs do not (1) prevent a required safety function from being achieved when needed during a DBE, or (2) result in a plant transient event not previously analyzed.

However, it is important to distinguish between categories of failures that (1) are required to be addressed within the design basis of a plant and (2) failures (i.e., CCFs) that are considered beyond design basis, which are the focus of this review guidance. Based on the characteristics of each type of failure, different methods are used for addressing their possible effects on the accomplishment of required safety functions and for defending against them.

Failures required to be addressed within the Design Basis include the following:

- cascaded effects from possible random hardware failures
- effects of faults propagated through system interconnectivity
- effects of faults resulting from failures occurring within shared resources

These types of failures are considered single failures per 10 CFR 50.55(a)(h) (IEEE-279 or IEEE-603) and must be evaluated and addressed within the design basis. The susceptibility of a proposed design to the above failure sources may be identified during the design and development process through careful performance of failure modes and effects analysis, fault tree analysis, and other forms of analysis of proposed designs (e.g., systems theoretic process analysis). Where identified, careful design evaluation processes and the application of defensive design measures should be used to preclude their occurrence or to limit the consequences of their occurrence to the point where a CCF occurring due to that vulnerability no longer presents an adverse consequence. Since 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; the use of traditional design basis considerations and conservative analysis methods is required.

Within integrated DI&C systems, random hardware failures can have cascading effects similar to effects of a CCF (e.g., loss of multiple functions within a safety group, spurious operation of functions within multiple safety groups). 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, "Application of the Single-Failure Criterion to Safety Systems," provides guidance for the deterministic analysis of single failures in systems required to perform safety functions. SRP Section 7.7, "Control Systems," provides guidance for the analysis of postulated failures in non-safety related (NSR) systems.

Failures to be considered as Beyond Design Basis CCF include the following:

- CCFs resulting from latent hardware or software defects leading to loss of function
- CCFs resulting from latent hardware or software defects leading to spurious operation of components or systems.

Beyond Design Basis failures, the subject of this document, are evaluated in a manner consistent with the SRM to SECY-93-087. The effects and consequences of these failures are not possible to decisively predict in advance through traditional design analysis methods and need to be addressed differently from the methods identified for Design Basis failures. If such a possible CCF cannot be prevented, eliminated, or mitigated through the design and development process, the consequences of the CCF should be evaluated and the consequences must remain acceptable within the plant design basis limits.

This document provides guidance for the evaluation of proposed DI&C designs that address defense in depth for CCF occurrences due to latent defects. Section B.2 of this BTP identifies an example of a general framework for a graded approach toward categorizing systems according to their safety significance. Section B.3 identifies guidance for possibly eliminating CCFs from further consideration, or for systematically limiting, mitigating, or coping with the effects of such CCFs resulting from possible latent software or hardware defects. Section B.4 provides guidance for evaluating qualitative assessment intended for modifications to structures, systems, and components (SSCs). Section B.5 discusses guidance for evaluating licensee or applicant evaluations of the effects of CCFs resulting from spurious operations. Section B.6 describes guidance for evaluating manual system level actuation and indications to address Item 18, Position 4, of Staff Requirements Memorandum (SRM)-SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," dated July 21, 1993. This document provides references to relevant review guidance for design and human factors considerations to be observed when addressing CCF in digital systems considered as design-basis events.

#### Defense-in-Depth Philosophy

In NUREG-0493, "A Defense-in-Depth and Diversity Assessment of the RESAR-414 Integrated Protection System," issued March 1979, documented a defense-in-depth and diversity (D3) assessment of a digital computer-based reactor protection system (RPS) which based defense against software CCF, which resulted in loss of a safety function during a DBE, upon an approach using a specified degree of system separation between echelons of defense. The RESAR-414 protection system consisted of the reactor trip system (RTS) and the engineered safety feature (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 the potential for CCFs occurring in digital systems used in NPPs.

The process of evaluating vulnerabilities of DI&C systems or components to possible CCFs is set within a framework of NPP safety analysis based on the principles of defense in depth. NPP control is modeled as a series of successive layers of defense, (referred to as "echelons of

defense”) each of which would need to be defeated for the consequences of a failure due to CCF to be able to cause unacceptable harm to public health and safety. Defense-in-depth design is essential to a regulatory structure that is designed to provide for reasonable assurance of adequate protection of public health and safety. In NPPs, the concept of control system defense-in-depth is modeled as the following echelons of defense for I&C systems (from NUREG/CR-6303, “Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems,” issued December 1994):

- Control System - The control system echelon usually consists of equipment that is not safety-related that is used in the normal operation of an NPP and routinely prevents operations in unsafe regimes of NPP operations.
- Reactor Trip System - The RTS echelon consists of safety-related equipment designed to reduce reactivity rapidly in response to an uncontrolled excursion.
- Engineered Safety Features - The ESF echelon consists of safety-related equipment that removes heat or otherwise assists in maintaining the integrity of the three physical barriers to radioactive release (cladding, vessel and primary cooling system, and containment) and the logic components used to actuate this safety-related equipment, usually referred to as the ESF actuation system, and controls.
- Monitoring and Indicator System - The monitoring and indicator system echelon consists of sensors, safety parameter displays, data communication systems, and independent manual controls relied upon by operators to respond to NPP operating events. The monitoring and indication system, along with system-level manual control actuation systems, is independent of the three other echelons of defense, such that no monitoring or system-level actuation equipment relied upon for operator response to events is vulnerable to failure due to a cause that is common to that of one or more of the other echelons.

If the normal plant control systems fail to perform their required functions to prevent operations in unsafe regimes of NPP operations, the next protective layer is the RTS, which will provide protection to prevent uncontrolled excursions and accidents from occurring. If accidents were to occur, the ESF systems are designed to mitigate their consequences. All of these systems are backed up by plant operators using the monitoring and indicator system to independently acquire the data necessary to manually perform required safety functions.

As licensees and applicants began proposing the use of DI&C systems within the echelons of defense when applying for certification of evolutionary and advanced light-water reactor designs, the NRC staff documented its position on vulnerabilities to CCFs in DI&C systems and outlined the need for assessing the adequacy of D3 in Item II.Q of SECY-93-087, dated April 2, 1993. The Commission subsequently modified this position in Item 18 of SRM- SECY-93-087, in which the Commission indicated that events associated with the triggering of CCF vulnerabilities due to software defects of a DI&C system are considered beyond DBE, and the evaluation of such events should use best-estimate methods.

The NRC staff provided plans to the Commission to clarify the guidance associated with addressing CCF vulnerabilities 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 reevaluation of the SRM for 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 SRM - SECY-93-087. These principles provide a framework for addressing CCF vulnerabilities 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 considers CCF vulnerabilities due to software and hardware defects in DI&C systems to be beyond design basis failures, applications and amendments proposing digital safety systems should include an evaluation of possible CCF vulnerabilities due to latent defects in DI&C systems. They should verify that the NPP defense-in-depth is adequate to protect the plant from the effects of these CCFs if they were to occur. In the event that the overall defense-in-depth posture is found to be not adequate, licensees or applicants should identify compensatory means to limit, mitigate, or cope with such possible CCFs. In addition, the application should include an evaluation of sources of this CCF vulnerability that can result in spurious operations, some of which may be considered within the design basis, as discussed later in this BTP.

After addressing single failures resulting in cascaded effects through design analysis methods, the remaining CCF vulnerabilities due to possible latent defects or spurious operations needs to be evaluated. The system performance under all expected modes of operation with the presence of possible latent defects should be evaluated. The effects of CCF vulnerabilities should be considered for their potential effects on all echelons of defense, to ensure that overall there is sufficiency in defense-in depth to assure the critical safety functions will be achieved, when needed, through automatic or manual means.

Based on the system architecture and the portion of the safety system to be replaced or installed, applicants and licensees should consider the application of limiting, mitigative, or coping measures to be used to address the remaining CCF vulnerabilities. Section B.3 describes this approach in detail.

Over the years, the NRC staff has approved applications with numerous design solutions, and in some cases, multiple design solutions applied within different parts of a single DI&C system, to address CCF vulnerabilities in DI&C systems. During these reviews, the NRC staff has observed that a number of solutions are successful in addressing CCF vulnerabilities, and that one standard solution may not be applicable to all DI&C systems. This BTP provides guidance for NRC technical staff to evaluate various acceptable methods licensees and applicants may have employed within proposed digital system design analyses addressing CCF vulnerabilities due to latent software and hardware defects and spurious operations in DI&C systems.

## 1. Regulatory Basis

The regulations listed below may not necessarily apply to all applicants and licensees. The applicability of the regulatory requirements is determined by the plant-specific licensing basis and any proposed changes to the licensing basis associated with the proposed DI&C system under evaluation:

- For NPPs with construction permits (CPs) issued before January 1, 1971, Title 10 of the *Code of Federal Regulations* (10 CFR) 50.55a(h) requires compliance with the plant-specific licensing basis IEEE Std 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," and the IEEE Std 603-1991 correction sheet dated January 30, 1995.
- For NPPs with CPs issued between January 1, 1971, and May 13, 1999, 10 CFR 50.55a(h) requires compliance with the requirements stated in IEEE Std 279-1968, "Proposed IEEE Criteria for Nuclear Power Plant Protection Systems"; IEEE Std 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations"; or IEEE Std 603-1991 and the correction sheet dated January 30, 1995.
- For applications for CPs, operating licenses (OLs), combined licenses (COLs), standard design approvals (SDAs), or design certifications (DCs) filed after May 13, 1999, 10 CFR 50.55a(h) requires compliance with IEEE Std 603-1991 and the correction sheet dated January 30, 1995.
- 10 CFR Part 50, "Domestic licensing of production and utilization facilities," Appendix A, "General Design Criteria for Nuclear Power Plants," General Design Criterion (GDC) 22, "Protection System Independence," requires, in part, that the protection system design shall ensure the following:

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 ... 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 the potential for CCFs 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.

- 10 CFR Part 50, "Domestic licensing of production and utilization facilities," Appendix A, "General Design Criteria for Nuclear Power Plants," GDC 24, "Separation of protection and control systems" states in part that interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired.
- 10 CFR Part 50, "Domestic licensing of production and utilization facilities," Appendix A, "General Design Criteria for Nuclear Power Plants," GDC 25, "Protection system

requirements for reactivity control malfunctions” states that the protection system shall be designed to assure that specified acceptable fuel design limits are not exceeded for any single malfunction of the reactivity control systems, such as accidental withdrawal (not ejection or dropout) of control rods.

- 10 CFR Part 52, “Licenses, certifications, and approvals for nuclear power plants,” governs applications for early site permits, DCs, COLs, SDAs, and manufacturing licenses (MLs) for nuclear power facilities.
- 10 CFR Part 100, “Reactor site criteria,” provides guideline values for fission product releases from NPPs licensed to operate before January 10, 1997, for which the licensee has voluntarily implemented an alternative source term under the provisions of 10 CFR 50.67, “Accident source term.” These guideline values can be commonly referred to as the site dose guideline values and provide the acceptance criteria for radiological release limits to bound the consequences of a CCF concurrent with a DBE.
- 10 CFR 50.67 provides guideline values for fission product releases from currently operating NPPs for which the licensee has implemented an alternative source term.
- 10 CFR 50.69 provides a risk-informed categorization and treatment of structures, systems and components for nuclear power reactors, and expectations for alternate treatment of those structures, systems and components in different risk categories.
- 10 CFR 50.34(a)(1)(ii)(D) provides site dose guideline values for CP applications filed under 10 CFR Part 50 after January 10, 1997.
- 10 CFR 52.47(a)(2)(iv) provides site dose guideline values for standard DC applications.
- 10 CFR 52.79(a)(1)(vi) provides site dose guideline values for COL applications.
- 10 CFR 52.137(a)(2)(iv) provides side dose guideline values for SDA applications.
- 10 CFR 52.157(d) provides site dose guideline values for ML applications.

## 2. Relevant Guidance

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

- NUREG/CR-6303 summarizes several D3 analyses performed after 1990 and presents a method for performing such analyses. NUREG/CR-6303, presents an analysis method that postulates common -mode failures<sup>1</sup> that could occur within digital reactor protection

---

<sup>1</sup> It should be noted that while these documents use the term “common-mode failure,” the BTP uses the term “common-cause failure” because it better characterizes this type of failure.



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 and strategies after a D3 assessment has been performed and it is determined that diversity in a given safety-related system is needed for mitigating potential vulnerabilities that can lead to a CCF. NUREG/CR-7007 identifies and develops a baseline set of diversity criteria that may constitute appropriate mitigating diversity strategies to address potential vulnerabilities to CCFs. While this NUREG describes a method for quantitatively assessing the amount of diversity in a system, this method has not been benchmarked and should not be used as the sole basis for justifying adequate diversity.
- SECY-93-087, Item II.Q, as clarified by SRM-SECY-93-087, Item 18, describes the NRC position concerning mitigation of potential common mode failures.
- SECY-18-0090, provides the NRC staff's plan to clarify the guidance for evaluating and addressing potential CCFs of DI&C systems.
- Generic Letter (GL) 85-06, "Quality Assurance Guidance for ATWS Equipment That Is Not Safety-Related," dated April 16, 1985, provides quality assurance guidance for anticipated transient without scram (ATWS) equipment that is NSR and as such may be used to demonstrate the quality of equipment that is NSR and credited for providing the diverse means to mitigate potential CCFs.
- RG 1.62, "Manual Initiation of Protective Actions," describes a method that the staff considers acceptable for use in complying with the NRC's regulations with respect to the means for manual initiation of protective actions provided (1) by otherwise automatically initiated safety systems or (2) as a method diverse from automatic initiation.
- 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 Section 7.7, provides review guidance for addressing the potential for inadvertent (i.e., spurious) operation signals from control systems.
- NUREG-0800, SRP Section 7.8, "Diverse Instrumentation and Control Systems," describes the review process and additional acceptance criteria for diverse I&C systems provided to protect against the potential for CCFs.
- NUREG-0800, SRP Chapter 18, "Human Factors Engineering," defines a methodology, applicable to both existing and new reactors, for evaluating manual operator action as a

diverse means of coping with AOOs and PAs that are concurrent with a CCF due to latent defects that disables a safety function credited in the SAR. SRP Chapter 18, Attachment A, provides a methodology for evaluating manual actions credited with the accomplishment of functions important to safety.

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

### 3. Scope

The guidance of this BTP is intended for staff reviews of I&C safety systems with (1) proposed modifications that require implementation of a license amendment, and (2) applications for CPs, OLs, COLs, DCs, SDAs, and MLs. This BTP is not applicable to proposed modifications performed under the change process in 10 CFR 50.59, “Changes, tests and experiments.”

### 4. Purpose

This document provides guidance for evaluating any D3 means credited to address vulnerabilities to CCF caused by latent defects in system hardware, software or software-based logic, as well as, the effects of any unmitigated CCF outcomes on plant safety. This BTP also provides staff guidance for reviewing a licensee or applicant’s graded approach, if used, to address CCF vulnerabilities in systems of differing safety classification.

In this guidance, software includes software, firmware,<sup>2</sup> and logic developed from software-based development systems (e.g., hardware description language programmed devices). As described above, events associated with this type of CCF vulnerability are considered beyond DBE, in accordance with Commission direction in SRM to SECY 93-087.

Further, this BTP provides guidance for reviewing (1) proposed design attributes, such as the use of diverse equipment, testing, or NRC-approved defensive measures incorporated within the design of a system or component to eliminate the potential for CCF from further consideration,<sup>3</sup> (2) diverse external equipment, including manual controls and displays to limit or mitigate a potential CCF, and (3) other measures to ensure conformance with the NRC’s position on addressing potential CCFs in DI&C systems as specified in SRM-SECY-93-087 and SECY-18-0090. The objectives of this review are to enable staff reviewers to verify the following with regard to licensee and applicant proposed DI&C safety systems:

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

---

<sup>2</sup> 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.

<sup>3</sup> Section B.3.1 of this BTP describes how a potential CCF is eliminated from further consideration.

- For DI&C systems of high safety significance, an adequate D3 assessment has been conducted that meets the acceptance criteria described in this BTP. An adequate D3 assessment consists of all of the following:
  - an evaluation of vulnerabilities to a CCF due to latent defects in system and the effectiveness of any credited attributes to eliminate the potential CCF from further consideration
  - identification and evaluation for effectiveness of any measures credited by licensees or applicants to (1) limit the consequences of CCFs to within acceptable levels, (2) mitigate CCF vulnerabilities that have not been eliminated from further consideration or (3) cope with the consequences of CCFs
  - an assessment of the effects associated with residual CCF vulnerabilities that have not been either eliminated from further consideration or limited/mitigated in some manner. This assessment should demonstrate that the consequences of the residual CCF remain acceptable.
- The results of a qualitative assessment of the vulnerability to CCF for proposed DI&C systems of lower safety significance meet the acceptance criteria within this BTP.

This BTP also addresses the applicant's assessment of vulnerabilities to a CCF due to latent software or hardware defects that can cause the spurious operation of a safety-related component or a component that is NSR. Adverse consequences of spurious operations due to CCF vulnerabilities are more likely to occur when systems or functions are highly integrated technology. Such 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 and must be included within the design basis and addressed in the plant safety analysis. This BTP provides criteria for reviewing an applicant's assessment of CCF vulnerabilities in DI&C systems that can result in spurious operation of safety-related components or components that are NSR.

## **B. BRANCH TECHNICAL POSITION**

### **1. Introduction**

#### **1.1. Four Common-Cause Failure Positions and Clarification**

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

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

Position 2 In performing the assessment, the vendor or applicant shall analyze each postulated

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

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

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

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- 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 the application adequately addresses vulnerabilities to potential CCFs. The guiding principles within SECY-18-0090 clarify that it is acceptable to use a graded approach commensurate with the safety significance of the proposed DI&C system or component to determine the degree of rigor necessary to address CCFs. Section B.2.1 of this BTP describes an example graded approach that may be used by licensees and applicants. The categorization scheme proposed by applicants and licensees should account for their plant-specific licensing basis and risk insights that are determined through the plant probabilistic risk assessment (PRA), where feasible.

The term “best estimate methods” in Position 2 is now referred to as methods using “realistic assumptions,” which are defined as the initial plant conditions corresponding to the onset of the event being analyzed. Initial plant event conditions include 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 that, in addition to “best estimate methods” (i.e., “realistic assumptions”) identified in Position 2 of SRM on SECY-93-087, Item 18, the D3 assessment can be performed using a design-basis analysis (i.e., 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 is based. Each event analyzed within the accident analysis should be evaluated in the D3 assessment independently. For example, if the initiating event is the loss of offsite power, the assessment does not need to assume another concurrent DBE.

If the D3 assessment shows a postulated CCF resulting from a software or hardware defect could disable a safety function (i.e., become a CCF), then Position 3 directs the assessment to identify an existing diverse means or add a diverse means to perform the safety function or a different function. The diverse means may be equipment that is NSR with a documented basis that the diverse means is of sufficient quality and not subject to the same CCF vulnerability. Examples of such demonstration of sufficient quality include alternate treatment requirements developed for implementation of 10 CFR 50.69, or GL 85-06, which provides quality assurance guidance for ATWS. SECY-18-0090 clarifies that use of either automatic or manual actuation within an acceptable time frame is an acceptable means of diverse actuation. SECY-18-0090 also specifies that if the D3 assessment demonstrates that a possible CCF, when evaluated in the accident analysis can be reasonably mitigated through other means (such as through the use of other installed systems), a diverse means that performs the same or a different function may not be needed. For example, an ATWS system may be credited as the diverse means, provided it is not subject to the same source of CCF vulnerability that disabled the safety function.

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

Position 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 and diverse from any vulnerability to a CCF identified within the "safety computer system" discussed in Positions 1 and 3 above and meets divisional independence requirements as applicable for the specific design implementation. While SRM-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-level actuation and control of equipment to manage the "critical safety functions" (see Section B.1.2). Further, if not subject to the same CCF vulnerability as the proposed safety-related DI&C system, some of these displays and manual controls from Position 4<sup>4</sup> may be credited as all or part of the diverse means provided to address Position 3.

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

---

<sup>4</sup> SECY-18-0090 did not provide any clarification for Position 4.

The four positions from SRM-SECY-93-087, acknowledge that DI&C system development errors (i.e., latent defects) are a credible source of CCFs. 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 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.

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 CCFs that can challenge plant safety. This includes CCFs 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 potential CCFs, the NRC staff should verify that for each event analyzed in the accident analysis section of the SAR, the license application or amendment request has done all of the following:

- 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 unacceptable consequences
- demonstrated that a CCF vulnerability due to 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
- 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 potential CCFs that have not been shown to be prevented, limited to within acceptable consequences, or mitigated.

## 1.2. Critical Safety Functions

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

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

Therefore, a safety function identified in the SAR may not always be a “critical safety function,” as defined in SRM-SECY-93-087. NUREG-0737, Supplement No. 1, “Clarification of TMI Action Plan Requirements: Requirements for Emergency Response Capability,” issued January 1983, provides additional guidance on critical safety functions and conditions.

## 2. Graded Approach and Level of Integration for Addressing Common-Cause Failure

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

Generally, the NRC staff can analyze the effects of CCFs on equipment credited with performing safety functions, and assessed in the SAR, using the criteria and guidance in NUREG/CR-6303. For safety systems, especially for those that do not have an imposed diversity requirement (e.g., through GDC), NUREG/CR-6303 describes one acceptable means to demonstrate adequate defense in depth. Since not all systems in the facility perform the same level of safety-significant protection functions, the assessment to evaluate consequences of CCF need not be standard. For example, systems that perform protection functions (e.g., RTS) are more critical than those that perform auxiliary safety functions that are not directly credited in the Chapter 15 analysis in the final SAR. Therefore, the degree of rigor associated with the assessment should be commensurate with the safety significance of the system. For example, the rigor of an assessment of CCF for a digital RTS would be expected to be more rigorous than that of assessment of CCF for a safety related MCR heating, ventilation, and air conditioning chiller. While the MCR heating, ventilation, and air conditioning chiller is a safety system that maintains certain temperature and humidity in the MCR for equipment and personnel to operate properly, a failure of this system would not have the immediate significant effects as would the failure of the RTS, because operators will have operating procedures or diverse or backup means to control temperature and humidity in the MCR and will exercise them or shut down the plant, if necessary.

This BTP provides a suggested framework for a possible graded approach toward categorizing systems according to their safety significance. Table 2-1 provides as an example. Once the SSC category is established and documented, this graded approach describes the level of rigor of the assessment that is to be applied to address CCF for the proposed DI&C system. Licensees and applicants are not required to use this approach. Non-graded approaches may be implemented at the discretion of the license or applicant.

**Table 2-1: Example Categorization Scheme for Implementing a Graded Approach to Evaluating the Consequences of Potential CCFs**

	Safety Related Equipment	Non-safety-Related Equipment
<b>Safety Significant</b> A significant contributor to plant safety	<p><b>A1 DI&amp;C SSCs</b></p> <p>Equipment relied upon to initiate and complete control actions essential to maintain plant parameters within acceptable limits established for a DBE or that maintains the plant in a safe state after it has reached safe shutdown state.<sup>5</sup></p> <p><b>or</b></p> <p>Failure could directly lead to accident conditions that may cause unacceptable consequences (e.g., exceeds siting dose guidelines for a DBE) if a) no other automatic A1 systems are available to provide the safety function or b) no pre-planned manual operator actions have been validated and credited to provide the required safety function.</p> <p><b>or</b></p> <p>Equipment required to have diversity to the extent practical, per the GDCs</p> <p><b>Application or amendment should include a D3 assessment as described in Section B.3</b></p>	<p><b>B1 DI&amp;C SSCs</b></p> <p>Equipment that is capable of directly changing the reactivity or power level of the reactor in a manner whose failure could initiate an accident sequence, or in a manner that adversely affects the integrity of the safety barriers (fuel cladding, reactor vessel, or containment).</p> <p><b>or</b></p> <p>An analysis demonstrates that a failure may result in possible adverse impact on plant safety due to integration of multiple control functions into a single system. If adverse safety consequences are possible, the failure may need to be considered a new AOO and included in the D3 assessment or addressed by other means.</p> <p><b>or</b></p> <p>Equipment required to have diversity to the extent practical, per the GDCs</p> <p><b>Application or amendment should include a qualitative assessment as described in Section B.4</b></p>
<b>Not Safety Significant</b> Not a significant contributor to plant safety	<p><b>A2 DI&amp;C SSCs</b></p> <p>Provides an auxiliary or indirect function in the achievement or maintenance of plant safety.</p> <p><b>Application or amendment should include a qualitative assessment as described in Section B.4</b></p>	<p><b>B2 DI&amp;C SSCs</b></p> <p>Equipment 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).</p> <p>Ex: An analysis demonstrates the failure does not have adverse impact on plant safety or can be detected and mitigated with significant safety margin.</p> <p><b>Application or amendment may need to include a qualitative assessment as described in Section B.4.</b></p>

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

<sup>5</sup> The plant safe shutdown state is site-specific, as defined in the nuclear facility’s licensing basis.



reasonably mitigated.”

The graded approach implemented by licensees and applicants should be consistent with the applicable licensing basis for the plant (e.g., principal design criteria (PDC) versus GDC) and risk insights available from the plant-specific PRA. Risk insights in terms of safety consequences from site-specific 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 a description of how the licensee or applicant applied any use of risk insights.

System integration and interconnectivity among the categories identified for the graded approach (as those shown in Table 2-1) can introduce additional vulnerabilities to sources of CCF. 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 proposed A1 system should consider the vulnerability to CCF resulting from failures within the integrated system and the consequences of a CCF that could affect the proper operations of the integrated or interconnected A1 systems. For example, if a digital protection system includes controllers for performing reactor trip and ESF logic as well as safety control functions (e.g., auxiliary feedwater level control), and the reactor trip or ESF initiation signal only reaches the final actuation device through the equipment that performs these safety control functions, then all the equipment in that pathway should be categorized A1. A D3 assessment should 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 these interconnected or integrated systems.

### 3. Defense-in-Depth and Diversity Assessment

Safety-related I&C systems should have adequate D3 to compensate for the occurrence of credible CCFs identified through the design analysis or postulated as defects within the design that are not possible to predict through a design analysis. A D3 assessment is a systematic approach to analyzing the proposed design of a safety system for credible failures that can occur concurrently within two or more independent divisions of a redundant design, leading to a failure of this system to perform its intended safety function when needed. Vulnerabilities of the proposed design to such CCFs could be assessed using a simple analysis or a more rigorous one, depending on the safety significance of the system. The D3 assessment also includes an analysis of the effects of CCFs that could occur to ensure that the consequences of the CCF are bounded within the limits deemed to be acceptable per the plant safety analysis.

A D3 assessment is necessary for a proposed A1 system or component to determine whether vulnerabilities to a CCF have been adequately addressed. If a non-graded approach is used, the D3 assessment must be performed for any system proposed within the application or amendment for staff evaluation. The licensee or applicant's evaluation should show that for each event analyzed in the accident analysis section of the SAR, the results of the D3 assessment indicates that vulnerabilities to CCF have been adequately addressed. The

consequences of any residual CCF vulnerabilities that have not been addressed must be evaluated and shown to be acceptable within the plant design basis.

### General Approach

The licensee or applicant's approach to providing defense against these vulnerabilities consist of performing a design analysis to determine whether there are any vulnerabilities to CCF in the design. If there are any vulnerabilities, there are a number of ways to address them:

- Vulnerabilities can be prevented or eliminated from further consideration using any of the methods described below:
  - use of diversity within the digital instrumentation and control system or component to eliminate a potential common-cause failure from further consideration, Section B.3.1.1
  - use of testing to eliminate potential common-cause failure from further consideration, section B.3.1.2
  - use of defensive measures to eliminate the potential for common-cause failure from further consideration, section B.3.1.3
- CCF vulnerabilities may be limited or mitigated by any of the design techniques described below:
  - crediting existing systems, Section B.3.2.1.
  - crediting manual operator action, Section B.3.2.2.
  - crediting a new diverse system, Section B.3.2.3.
- The consequences of CCF vulnerabilities may be analyzed and found to remain within acceptable limits for the AOO or PA associated with the CCF, per the acceptance criteria within Section B.3.3.

Once potential sources of CCF have been identified, and feasible design features for preventing, limiting, mitigating, or coping measures have been incorporated to address them, licensees and applicants need to reassess the effects of any remaining (residual) risk. This requires an evaluation of the adequacy of the measures that have been incorporated into the design, to demonstrate that there is now reasonable assurance of adequate protection in the presence of residual risk from sources of CCF.

This general approach may be applied not only for identifying solutions for addressing CCF for the entire system, but applicants may select different strategies for addressing CCF for different portions of the system. For example, the applicant may show that the CCF vulnerability has been successfully eliminated from further consideration for a component within the system but exclude the use of this component when addressing the CCF vulnerabilities for the rest of the system. Also, different vulnerabilities may require multiple strategies to be applied to reduce the likelihood. For example, for a portion of the system, design measures can be used to eliminate or reduce the likelihood of the CCF; in other portions the CCF vulnerability may be mitigated by relying on other I&C system(s). This assessment depends on the facility type and the facility's design and design bases. Further the vulnerability needs to be analyzed on an

accident event-by-event basis, which can result in different solutions applied to address CCF.

The adequacy of the D3 assessment should be justified, including any (1) measures used to eliminate the potential CCF from further consideration, (2) means provided to mitigate the CCF, or (3) analysis to show the consequences of the CCF are acceptable for each DBE; the NRC staff's safety evaluation should explicitly address these same areas.

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

Many system design and testing attributes, procedures, measures, and practices can contribute to significantly reducing the likelihood of a CCF from occurring. However, certain design attributes are sufficient to eliminate from further consideration a potential CCF due to a digital design or implementation defect. These attributes include: (1) diversity within the DI&C system or component, (2) testability, and (3) other NRC-approved defensive measures within the design. If the application demonstrates that the use of these design attributes, in any combination or on their own, for a system or component meets the criteria within this BTP, the potential CCF will be effectively eliminated from further consideration.

Although these attributes do not eliminate the CCF vulnerability completely, the consequence of a CCF occurring is minimized such that no further evaluation is necessary. The following sections discuss the basis for the acceptability of each attribute. 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 system does not need to be performed for the portion of the system or component that credits these attributes.

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

Diversity within the I&C system or component constitutes schemes, features, or additions to eliminate the possibility of a CCF. Diversity can be implemented by using different technologies, algorithms or logics, sensing devices, or actuation devices. However, diversity needs to be paired with independence, otherwise the diverse means could be susceptible to the same vulnerability. Section 2.6 of NUREG/CR-6303 identifies six diversity attributes and 25 related diversity criteria that licensees and applicants can use. NUREG/CR-7007 identifies and develops a baseline set of diversity criteria that may constitute appropriate mitigating diversity strategies to address vulnerabilities to CCFs.

If sufficient diversity in performance of the safety function exists within each safety division or among redundant safety divisions of a system, then the potential CCF can be eliminated from further consideration. For example, a digital protection system could be designed such that each credited safety function is implemented in one division of the protection system that uses one type of digital technology and another division that uses a different type of digital technology.

Staff reviewers should verify that the application includes an analysis using 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 such that further consideration is unnecessary. Given that this analysis is qualitative in nature, the potential that a CCF can affect both diverse systems or divisions is minimized but not eliminated.

### Acceptance Criteria

The reviewer should reach a conclusion that the application provides adequate information on the use of diversity within the system or component to eliminate CCFs from further consideration, if the application demonstrates that the following acceptance criteria are met:

- a. Each safety function to be achieved by the proposed design is shown to be independently achievable by each diverse portion in the system.
- b. An analysis demonstrates that adequate diversity has been achieved between the diverse portions of the system or component in accordance with the guidance of NUREG/CR-6303 and NUREG/CR-7007. Diversity in the accomplishment of the required safety function is deemed adequate if the safety function can be accomplished independently by each set of diverse equipment and software without reliance on the performance of common components, and the equipment and software of each diverse portion are not subject to the same sources of CCF.
- c. The diverse portions of the system or component do not have common or shared resources, such as power supplies, memory, bus, or communications modules that could affect both portions. The diverse portions of the system or component do not share engineering or maintenance tools that could affect both portions.
- d. Each diverse portion used to perform the credited safety functions is shown to be highly reliable and continually available for the plant conditions during which the associated event is expected to be prevented or mitigated.
- e. Periodic surveillance criteria are used to verify the continued operability of each diverse design.
- f. Consistency is maintained between the proposed change and technical specifications.

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

When considering CCF vulnerabilities in DI&C systems or components, there are two general areas of concern: (1) CCF resulting from errors introduced by the system hardware or software design, and (2) CCF as a result of errors or defects introduced during the implementation or fabrication of the software, hardware, or software--based logic. A high-quality development process, in conjunction with rigorous system analysis (e.g., failure modes and effects analysis, system theoretic process analysis) can be used to address many potential design errors in the system or component requirements or specifications for both analog and digital equipment.

However, even a high-quality development process cannot completely eliminate potential latent defects introduced during the design and implementation process.

Rigorous testing can help to identify latent defects in the design, fabrication, and implementation of software or software-based logic, provided a design is simple enough to enable such testing. Testing can be used to uncover latent defects for correction in the design, fabrication, and implementation process, and to demonstrate that any identified latent defects have been corrected. If testing of a proposed component shows that there are no latent defects of the component software or software-based logic, the CCF can be eliminated from further consideration.

The set of test cases applicable to systems with a large number of inputs, even with only a small amount of memory, can become impracticably large. The testing approach outlined 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 all expected operational modes and conditions of the proposed 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, staff reviewers should verify that the application demonstrates that any credited testing process incorporates all of the following concepts:

- a. A programmable digital device (PDD) is not considered susceptible to CCF if it can be shown to be deterministic in performance, has documentation of all expected performance for each of its functional modes of operation, and for all transitions between its various functional modes of operation, and is testable based on the following criteria:
  - testing every possible combination of inputs including every possible sequence of inputs
  - for PDDs that include analog inputs, the testing of every combination of inputs include the entire operational range of the analog inputs, (including defined over-range and under-range conditions)
  - testing every possible executable logic path (this includes nonsequential logic paths)
  - testing every functional state transition among all modes of operation
  - conformance to preestablished test cases to monitor for correctness of all outputs for every case.
- b. This testing is to be conducted on the PDD integrated with test hardware accurately representing the performance of the target hardware.
- c. It is possible that PDDs could include unused inputs. If those inputs are forced by the module circuitry to a desired known state, that can be accounted for in the test cases, those inputs can be excluded from the “every combination of inputs” criterion. There may be more than one desired safe state depending on the mode of operation of the plant and of the PDD. The staff reviewer should verify that designers of systems using

PDDs have taken this into account when designing the PDD and when identifying the appropriate set of test cases.

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 adequate information on the test results and testing methodology for a device or component such that a potential CCF can be eliminated from further consideration, if the application demonstrates that all of the following acceptance criteria are met:

- a. The proposed design has documentation of all expected performance for each of its functional modes of operation, and for all transitions between its various functional modes of operation, and is testable based on the following criteria:
  - testing every possible combination of inputs, including every possible sequence of inputs
  - for PDDs that include analog inputs, testing every combination of inputs includes the entire operational range of the analog inputs, (including defined over-range and under-range conditions)
  - testing every possible executable logic path (includes nonsequential logic paths)
  - testing every functional state transition among all modes of operation
  - conformance to preestablished test cases to monitor for correctness of all outputs for every case
- b. The testing for latent defects was conducted on the PDD integrated with test hardware accurately representing the hardware to be installed, such that the installed hardware will perform the same as the corrected test hardware.
- c. If the PDD included has unused inputs, and if those inputs are forced by the module circuitry to a desired known state accounted for in the test cases, those inputs may be excluded from the “every combination of inputs” criterion.

#### 3.1.3. Use of Defensive Measures to Eliminate the Potential for Common-Cause Failure from Further Consideration

Defensive measures may be used to prevent, eliminate from further consideration, limit, or mitigate the effects of a CCF vulnerability. However, if the application credits the use of NRC-approved defensive measures to eliminate the potential for a CCF from further consideration, the application should include the following:

- a. an identification of the source of vulnerabilities or hazards for which the NRC-approved defensive measures are being applied
- b. a description of the NRC-approved defensive measures being credited to address the identified vulnerabilities or hazards
- c. a description of how the CCF vulnerability will be prevented, or its consequences 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 will be limited, mitigated, or prevented, including an analysis of how the effectiveness of the measures credited can be demonstrated
- e. an assessment of the consequences of any residual risks from CCFs showing how the residual risk has been bounded within the allowable limits of the safety analysis

### Acceptance Criteria

The reviewer should reach a conclusion that the application provides sufficient information on the credited defensive measures to eliminate a potential CCF from further consideration if the application includes the documented supporting technical basis and acceptance criteria to demonstrate that these defensive measures are based on an NRC-approved methodology. If the application includes a technical basis and acceptance criteria, the NRC staff will review the information on a case-by-case basis.

### 3.2. Use of Diverse Means to Mitigate Common-Cause Failures

If a potential CCF vulnerability has not been eliminated from further consideration using the process in Section B.3.1 of this BTP, a diverse means should be provided to accomplish the same or different function than the safety function disabled by the postulated CCF. Section 2.6 of NUREG/CR-6303 identifies six diversity attributes and 25 related diversity criteria that can be used to support a qualitative analysis. NUREG/CR-7007 identifies and develops a baseline set of diversity criteria that may constitute appropriate mitigating diversity strategies to address vulnerabilities to CCFs.

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

- a. Any credited existing system(s) is capable of effectively performing the same or a different function in response to the DBE, which has the same safety objective as the system under evaluation

- b. Any manual operator action(s) credited in the D3 assessment can be implemented 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
- c. Any new credited diverse system(s) is supported by instrumentation independent from the safety system and, therefore not subject to the same vulnerabilities, and that indicates all of the following:
  - whether the safety function is needed
  - whether the -system successfully performed or did not perform the safety function
  - whether the automated diverse means or manual operator action is successful in performing the design functions necessary to mitigate the CCF

### 3.2.1. Crediting Existing Systems

An existing reliable I&C system can be used as a diverse means to provide the same or a different function credited in the D3 assessment. The function performed by this existing I&C system should result in plant consequences that do not exceed the limits prescribed for each AOO or PA in the SAR. An analysis should be performed to demonstrate that the existing plant system to be credited and the proposed system are not subject to the same postulated CCF.

The existing system may be a system that is NSR provided it is of sufficient quality and can reliably perform the credited functions under the associated event conditions. NSR systems that are credited in the analysis that are in continuous use (e.g., the normal RCS inventory control system or normal steam generator level control system) are not required to be upgraded to meet augmented quality standards. NSR systems that are credited in the analysis that are not in continuous use (i.e., they are normally in standby mode) should be evaluated for reliability to demonstrate that the system will perform its intended function. For example, the plant ATWS system capabilities may be credited as a diverse means of achieving reactor shutdown, provided that the ATWS system to be credited is capable of responding to the same analyzed events as the proposed system. The ATWS system to be credited should (1) be diverse from the proposed DI&C system, (2) has been demonstrated to be highly reliable and of sufficient quality, and (3) be responsive to the AOO or PA sequences using independent sensors and actuators as the proposed DI&C system.

If equipment outside of the MCR, that is not subject to the same CCF vulnerability as the safety system, is used to perform the credited manual operator action, then the reliability, availability, and accessibility of the equipment under the postulated event conditions should be demonstrated. HFE principles and criteria identified in SAR Chapter 18 should be applied to the selection and design of the displays and controls.

### Acceptance Criteria

The reviewer should reach a conclusion that the application includes a D3 assessment justifying



the use of an existing plant system as the diverse means. The existing system could perform the same function disabled by the postulated CCF or to perform a different function to compensate for or mitigate the loss of the function disabled by the postulated CCF. The application should demonstrate the following:

- a. The equipment to be credited is highly reliable, of sufficient quality, and is expected to be available during the associated event conditions.
- b. The equipment to be credited is not subject to the same postulated CCF or sources of CCF as the proposed DI&C system.
- c. The equipment to be credited (1) has the capabilities of sensing and responding to the same plant conditions as the affected system if performing the same safety function, or (2) is capable of sensing and responding to alternative plant conditions if performing a different function. For both options, the application should show that the capabilities for sensing and responding maintain plant safety by verifying that plant conditions stay within the acceptance criteria specified for each AOO or PA in the SAR.

### 3.2.2. Crediting Manual Operator Action

When addressing Position 3 of SRM/SECY 93-087, manual operator actions can be credited as a diverse means to provide the same or a different function credited in the D3 assessment. To be creditable, manual actions should be performed within a time frame adequate to be effective in mitigating the event. Proposed manual actions must be shown by licensees and applicants to be both feasible and reliable, through a HFE process, such as the process outlined in SRP Chapter 18. A graded, risk-informed approach may be used by the staff to determine the appropriate level of human factors engineering review that should be applied in the staff's evaluation of proposed changes to existing credited manual operations or proposed new manual operations.

The equipment necessary to perform these actions, including the supporting indications and controls, should be diverse and independent from (i.e., capable of completing the protective action independently, and not vulnerable to the same sources of CCF as) the safety-related I&C system. If the equipment used to perform the credited manual operator action is NSR, then the application should include information to demonstrate that the equipment used is highly reliable and of adequate quality, such as alternate treatment requirements developed for implementation of 10 CFR 50.69, or GL 85-06 which provides quality assurance guidance for ATWS.

If equipment outside of the MCR, that is not subject to the same CCF vulnerability as the safety system, is used to perform the credited manual operator action, then the reliability, availability, and accessibility of the equipment under the postulated event conditions should be demonstrated. HFE principles and criteria identified in SRP Chapter 18 should be applied to the selection and design of the displays and controls.

### Protective Actions Initiated Solely by Manual Actions

Protective actions initiated solely by manual controls are subject to the consideration of appropriate HFE criteria and the use of adequate equipment and controls. RG 1.62 provides guidance for evaluating the adequacy of equipment and controls used as the means for manual initiation of protective actions provided by otherwise automatically initiated safety systems, or as a method diverse from automatic initiation. SRP Chapter 18, Attachment A, provides guidance for evaluating the adequacy of human factors reviews performed to validate the feasibility and reliability of the proposed manual actions.

### Acceptance Criteria

The reviewer may use the guidance within NUREG-1764, Revision 1, to perform a risk-informed evaluation of the licensee or applicant submittal. The reviewer should reach a conclusion that using the proposed manual operator action is acceptable provided the application demonstrates that the following acceptance criteria are met:

- a. The proposed manual operator actions have been validated using an HFE process as specified in SRP Chapter 18, Attachment A, and found to be both feasible and reliable. The application describes human performance requirements and relates them to the plant safety criteria. Recognized human factors standards and design techniques are employed to support the described human performance requirements.
- b. The equipment used to support manual operator action is independent and diverse from the automatic safety system, such that it is not subject to the same CCF vulnerabilities as the automatic safety system. The equipment credited is of sufficient quality, and is accessible during the associated event conditions, as described above.
- c. The indications and controls needed to support the manual operator action have the functional characteristics necessary to maintain the plant within the accepted limits.

#### 3.2.3. Crediting a New Diverse System

A new diverse system (e.g., diverse actuation system) 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 potential CCFs, 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 proposed system so that they are not subject to the same postulated CCF. An analysis should be performed to demonstrate that the diverse means to be credited and the digital design used for the proposed system are not subject to the same CCF vulnerability. 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 an NRS system, if the system is of sufficient quality to perform the necessary function(s) under the associated event conditions. The diverse means should be highly reliable and of adequate quality, such as alternate treatment requirements developed for implementation of 10 CFR 50.69, or GL 85-06 which provides quality assurance guidance for ATWS.

#### Prioritization

If a new diverse system is implemented, it will be necessary to ensure that signals to actuating components coming from the different systems are adequately prioritized to ensure the overall defense-in-depth strategy is maintained. If the proposed system and the new diverse system share resources (e.g. priority modules), the application should demonstrate that the proposed system has priority over the resources when it is operable and available. 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; this should be considered when developing a priority scheme.

#### Acceptance Criteria

The reviewer should reach a conclusion that using a new diverse system is acceptable provided the application demonstrates that 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.
- b. Sufficient diversity exists between the diverse system and the proposed system, so that they are not subject to the same postulated CCF.
- c. The equipment to be credited has functional capabilities sufficient to maintain the plant within the applicable acceptance criteria.
- d. Proposed system(s) or other systems/manual operator action that share common resources should have prioritization of commands consistent with the guidance in DI&C-ISG-04 and the licensing basis of the plant. The basis for the prioritization should be documented.
- e. If NSR equipment is used in the diverse system, the equipment is highly reliable and of sufficient quality to perform the necessary function(s) during the associated event conditions.

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

Once vulnerabilities to CCF are identified, licensees and applicants may use design measures to eliminate these vulnerabilities or include compensatory means to limit, mitigate, or cope with such possible CCFs. If licensees and applicants do not address these vulnerabilities or when

measures to prevent CCF cannot be used, the licensee or applicant should evaluate if the facility can operate and remain within its safety limits should these CCFs occur. The staff should verify that the evaluation demonstrates that consequences of the CCFs remain acceptable.

For each event analyzed in the 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 potential CCFs of a proposed system, or portions of a proposed system, are acceptable.

#### Acceptance Criteria

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

- a. For each AOO in the design basis occurring in conjunction with the CCF, the plant response calculated using realistic or conservative assumptions does not result in radiation release exceeding 10 percent of the applicable siting dose guideline values or violation of the integrity of the primary coolant pressure boundary.
- 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 due to latent defect (i.e. CCF) of a proposed modification of an SSC with digital technology. This methodology is referred to as a qualitative assessment. If a graded approach is implemented, the qualitative assessment may be applied to the graded categories as suggested in the example Table 2-1. The qualitative assessment is based on (1) a consideration of factors used to eliminate of CCFs from further consideration, and (2) the failure analysis (e.g., failure modes and effects analysis (FMEA), fault tree analysis). Taken together, these considerations provide adequate technical basis to demonstrate that CCF can be removed from further consideration in the overall defense-in-depth evaluation for purposes of this BTP.

First, 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 (i.e., low likelihood of CCF), such that likelihood of failure of the proposed DI&C system remains consistent with the previous assumptions in the licensing basis:

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

Second, as part of the qualitative assessment, supplementing failure analyses information from engineering design work such as FMEAs and FTAs can supplement the factors above by, for example, demonstrating that identified vulnerabilities to CCF are addressed. Also, best-estimate analyses may be performed to show that the potential consequences of postulated failures are bounded.

Consideration of these factors, as well as supplementing failure analyses information as described in RIS 2002-22, Supplement 1, is an acceptable method to address potential CCFs in A2, B1, and applicable B2 systems.

#### Acceptance Criteria

The reviewer should reach a conclusion that the application has addressed CCF vulnerabilities in A2, B1, or applicable B2 systems if the application provides a qualitative assessment that gives an adequate technical basis concluding that CCF can be removed from further consideration. The application should describe the following criteria:

- a. The proposed system has design attributes and features that reduce the likelihood of CCFs.
- b. The quality of the design process of the DI&C system reduces the likelihood of CCFs due to latent defects in the software or software-based logic in the DI&C system or component.
- c. The applicable operating experience on 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.
- 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).
- e. Failure analyses (e.g., FMEAs) and best-estimate analyses that demonstrate how failure effects are bounded or accounted for are documented.

## 5. Spurious Operation Due to Latent Defects

### Regulatory Basis

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

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

IEEE Std. 279-1971, (as incorporated by reference 10 CFR) 50.55a(h)) Clause 4.7.4 discusses scenarios involving multiple failures resulting from a credible single event.

SRP Section 7.7, "Control Systems" states, in part, that the control systems design should limit the potential for inadvertent actuation and challenges to safety systems. SRP Section 7.7 also states, in part, failure of any control system component or any auxiliary supporting system for control systems does not cause plant conditions more severe than those described in the analysis of anticipated operational occurrences.

### Background

As stated earlier in this BTP, latent defects, particularly latent defects in software are considered credible sources of CCF. One potential outcome of a CCF is the potential loss of ability of an SSC to perform its design function. However, another potential outcome of a CCF is the potential for an SSC to inadvertently actuate or initiate equipment operation without a valid demand or due to an erroneous signal. This is generally referred to as spurious operation (previously known as spurious actuation) for purposes of this BTP. A spurious operation can be detected (although not always anticipated) because this type of failure normally is self-announcing by the actuated system. However, there may be circumstances in which a spurious trip or actuation would not occur until a particular signal or set of signals are present. In these cases, the spurious trip or actuation would not occur immediately upon system startup but could occur under particular plant conditions. This circumstance is still self-announcing (by the actuated system,) even if the annunciation did not occur on initial test or startup.

Due to the potential consequences of a spurious operation, a failure of a system to actuate might not be the worst-case failure. This is true especially when analyzing the time required for identifying and responding to conditions resulting from spurious operation in an automated safety system. For example, a failure to trip might not be as limiting as a partial actuation of an emergency core cooling system, but with indication of a successful actuation. In such cases it may take an operator longer to evaluate and correct the safety system failure than it would if there was a total failure to send any actuation signal. Therefore, the evaluation of failure effects as a result of CCF may need to include both the possibility of partial (or full) actuation and failure to actuate with false indications, as well as a total failure to actuate in accordance with

Section 3 of NUREG/CR-6303 because failures of the automated protection system stemming from a CCF can cause spurious operation of plant equipment.

#### Spurious Operations due to different failure types

It is important to distinguish spurious operations that are required to be addressed within the design basis and spurious operations as a result of failures that are beyond design basis.

Spurious Operations required to be addressed as part of the design basis include:

- Spurious operations as a result of single failures (including cascading effects)
- Spurious operations as a result of single malfunctions

Consistent with regulatory requirements such as 10 CFR 50.55(a)(h) – (IEEE-279 or IEEE 603) and GDC 25, spurious operations as a result of single failures and single malfunctions are expected during with lifetime of the plant and are required to be addressed as part of the design basis. RG 1.53 provides guidance for the deterministic analysis of single failures in systems required to perform safety functions. SRP Section 7.7 provides guidance for the analysis of postulated failures in non-safety related systems.

Spurious Operations are beyond design basis if they result from failures such as:

- CCFs originating from latent hardware defects
- CCFs originating from latent software defects

Spurious operations originating from latent defects (i.e. CCF) are the focus of this BTP. As stated in the Background section of this BTP, beyond design failures (i.e. CCF due to latent defects) must be evaluated in a manner consistent with SRM to SECY 93-087. In addition, consistent with SRM to SECY 93-087, spurious operations as a result of latent defects are considered beyond design basis events and can be addressed using the methodologies described in this BTP at the discretion of the licensee or applicant, where appropriate.

#### Spurious Operation and Highly Integrated Systems

As stated earlier in this BTP, the ability to integrate design functions using digital instrumentation and control (DI&C) technology makes the identification of CCF vulnerabilities and evaluation of potential consequences of a postulated CCF challenging. System integration and interconnectivities including shared resources have the potential to reduce overall defense-in-depth (e.g. reduction in independence) for a plant. Therefore, with regard to spurious operation, the primary concern is with highly integrated digital systems and the potential for spurious operation of multiple functions due to a common latent defect.

Due to differences in regulatory requirements (e.g. independence and quality requirements) between safety-related SSCs and NSR SSCs, highly integrated NSR systems are of greater concern and should be the primary focus of this assessment for the reviewer. Numerous NSR

systems can directly or indirectly affect reactivity and in some cases (e.g. NSR rod control system) have failures previously analyzed in the design bases. A CCF of a highly integrated NSR system/platform (i.e. multiple NSR system functions controlled by the same platform) have the potential to place a plant in an unanalyzed condition. Note: the reviewer should also consider the level of integration between safety and NSR systems as a potential vulnerability to be addressed.

#### 5.1. Spurious Operation Assessment

Sections 3 and 4 of this BTP describes measures that can be taken to address potential CCF vulnerabilities in the proposed design, including those that can lead to spurious operation. The design and/or analytical solutions that address CCF vulnerabilities by preventing, eliminating or mitigating their effects would also address postulated spurious operation.

The effects of credible postulated spurious operation caused by a CCF in the digital protection system may not be evaluated in the existing plant accident analyses. In these cases, an analysis should be performed to determine whether postulated spurious operation could result in an unanalyzed plant condition. Further, the analysis can identify whether adequate coping strategies exist (or need to be developed) for these postulated spurious operation (e.g., emergency, normal, and diverse equipment and systems, controls, displays, procedures and the reactor operations team).

Note: Spurious operation is considered an initiating event only, without a concurrent DBE for purposes of this assessment.

##### Acceptance Criteria

Based upon the information provided in the application regarding spurious operations, the reviewer should reach a conclusion that the accident analysis results have not been invalidated due to potential spurious operations introduced by the design, or that previous spurious operation assumptions have not been affected by the design.

For example,

- a. Any defensive measures or design attributes implemented for a proposed system to eliminate the vulnerability to CCF from further consideration also demonstrate that spurious operations are eliminated. Section B.3.1 of this document provides acceptance criteria for evaluating defensive measures or design attributes..
- b. For those postulated spurious operations that have not been shown to be mitigated, or eliminated entirely, the consequences resulting from spurious operation of safety-related or non-safety related components are bounded by the events analyzed in the accident analysis in accordance with Section B.3.3 of this document. If not bounded, they are identified as new AOOs and analyzed



accordingly.

- c. Any automatic functions or manual operator action credited to mitigate the conditions caused by potential spurious operation of safety-related or non-safety related components meet the acceptance criteria within Section B.3.2 of this document.
- d. Any measures implemented to address the CCF vulnerability through a qualitative assessment for A2, B1 or B2 systems meet the acceptance criteria within Section B.4 of this document.

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

Displays and manual controls provided for compliance with Position 4 of SRM -SECY-093-87, Item 18, should be sufficient to both monitor the plant state and enable control room operators to actuate critical safety functions, as defined in Section B.1.2 of this BTP. RG 1.62 outlines important design criteria for DI&C equipment used by plant operators for the manual initiation of protective actions when addressing Position 4. Existing analog displays and controls in the MCR could satisfy Position 4. The same digital platform or analog technology should not be used for both mitigating the DBE and providing signals to these displays and controls to meet Position 4.

For displays and manual controls used to conform to Position 4, staff reviewers should verify that the following criteria have been met:

- a. The required minimum inventory of displays and 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 these critical safety functions should be at the system- or division-level and located within the MCR.
- c. Equipment that is NSR may be used for these manual controls and indications, provided the equipment is reliable and of sufficient quality. Examples of such demonstration of sufficient quality include alternate treatment requirements developed for implementation of 10 CFR 50.69, or GL 85-06 which provides quality assurance guidance for ATWS.
- d. The displays and controls used to address Position 4 shall be independent and diverse from the safety-related DI&C systems that are vulnerable to a CCF such that these display and controls are not affected by potential CCFs that could disable the safety-related DI&C systems.

Once system-level or division-level manual actuation from the MCR using the Position 4

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

### Acceptance Criteria

The reviewer should reach a conclusion that the manual controls and supporting indications conform to Position 4 of SRM-SECY-93-087, Item 18, if the application demonstrates that the following acceptance criteria have been met:

- a. Proposed manual actions credited to accomplish safety functions, that would otherwise have been accomplished by automatic safety actions, should be demonstrated to be both feasible and reliable through a human factors analysis as described in Chapter 18 of this SRP. Section 3.2.2 of this BTP presents the acceptance criteria. The application should sufficiently demonstrate minimum inventory of displays and controls for the operator to effectively monitor and initiate the accomplishment of critical safety functions, such that the plant remains within analyzed limits. Such manual operator actions should be prescribed by approved plant procedures and subject to appropriate training.
- b. The manual controls for these critical safety functions are at the system or division level and 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. If NSR equipment is used, the quality and reliability of the equipment are adequate to support the manual operator action during the associated event condition.
- d. The displays and controls are independent and diverse from the safety-related DI&C systems such that these displays and controls are not affected by postulated CCFs that could disable the safety functions performed by the safety-related DI&C systems.

## 7. Information To Be Reviewed

It may be necessary for the staff to perform a multidisciplinary review in cooperation with other NRC staff. The technical staff should review the following:

- a. the documentation of the categorization of 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, the PRA results should be reviewed.
- b. for an A1 system (or for a proposed system if the graded approach is not implemented), the results of the D3 assessment; specifically, the following:
  - identification of any design attributes credited to eliminate potential CCFs from further consideration and a demonstration that these attributes or measures are effective, and identification of any remaining vulnerabilities (residual risks) to potential CCFs
  - for CCFs that have not been eliminated using design attributes, identification of any diverse means provided to accomplish the same or a different function than the safety function disabled by a postulated CCF; if any diverse means are credited to mitigate the potential CCF, the NRC staff should review the information provided to demonstrate the effectiveness of the diverse means, including assessment from HFE analysis associated with manual operator action if used as a diverse means
  - for CCFs that have not been eliminated from further consideration, mitigated or limited using diverse means, or justified as being acceptable, identification of any analysis performed to demonstrate that consequences of a CCF are within acceptable limits for each AOO and PA; if any consequence analysis has been performed, the NRC staff should review the results of this analysis.
- c. if a graded approach is being implemented, for A2 and B1 systems, the results of the qualitative assessment of these systems, including the following:
  - information supporting the use of design attributes and features
  - information regarding the quality of the design and development process
  - information regarding applicable operating experience
  - supporting analyses and justification of assumptions
- d. if a graded approach is being implemented, for a B2 system, information to show that the proposed design will not introduce any conditions that are unbounded by the events in the accident analysis due to the specific implementation
- e. information on the results of the spurious operation assessment that describes at least one of the following, depending on whether a graded approach is being implemented:

- Potential spurious operations due to a CCF vulnerability 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
  - Potential spurious operations due to a CCF vulnerability in an A2, B1 or B2 system have been addressed through use of a combination of the three factors and supporting analyses described in Section B.4 of this BTP
  - The consequence of a potential spurious operation due to a CCF is bounded
- f. for a proposed system, design information showing that controls and displays have the following attributes:
- have been provided in the MCR to perform manual system or division level actuation of critical safety functions
  - are independent and diverse from the proposed system such that they are not subject to the same CCF as the proposed system
  - have sufficient quality to support the manual operator action during the associated event condition if the equipment used is NSR.

## 8. Review Procedures

In reviewing the D3 assessment results in accordance with the acceptance criteria described in Section B.3 of this BTP and the detailed guidance of NUREG/CR-6303 and NUREG/CR-7007, reviewers should focus on the topics described below.

### 8.1. System Representation as Blocks

The system being assessed is represented as a block diagram; the inner workings of the blocks are not necessarily shown. A block is 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, will not propagate to other equipment or software. A block can be a software macro or subroutine, such as voting block or proportional-integral-derivative block used by multiple functional applications; a design or implementation defect in this type of block can result in a CCF of all application functions that use that block. Diversity is evaluated at the block level.

Examples of typical blocks are computers, local area networks, software macros and subroutines, and programmable logic controllers.

### 8.2. Documentation of Assumptions

The staff reviewer should verify that the application or amendment documents 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 potential CCF. This includes the functions of blocks that act to prevent or mitigate consequences of the CCF under consideration.

### 8.4. Identification of Alternate Trip or Initiation Sequences

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

### 8.5. Identification of Alternative Mitigation Capability

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

When manual operator action is cited as the diverse means for response to an event, the applicant should demonstrate that the HFE analysis demonstrates that this action is both feasible and reliable in accordance with SRP Chapter 18. Such activity should include coordination with the organization responsible for the review of human-system interfaces for any credited diverse manual operator action.

### 8.6. Justification for Not Correcting Specific Vulnerabilities

Justification should be provided for not correcting any identified vulnerabilities that were unresolved by other aspects of the application such as design attributes (e.g., redundancy, diversity, independence), defensive measures, and the inclusion of diverse actuation or mitigation capability. This includes previously NRC-approved credited manual operator actions in the licensing basis to address AOOs or PAs. These justifications should be included within license applications and amendments, with sufficient supporting information so that the staff may review them on a case-by-case basis. For example, licensees or applicants may potentially credit the ability of plant operators to identify system leakage using the plant leak detection system prior to the onset of a large break pipe rupture. Justification for the crediting of such manual operator actions could be used with appropriate analysis of site-specific factors such as pipe configuration and design, piping fracture mechanics, leak detection system capabilities, and detailed manual operator actions and procedures, as appropriate. A multi-disciplinary staff review team should engage licensees or applicants in early pre-application meetings that may pursue this approach.

## C. REFERENCES

1. Institute of Electrical & Electronics Engineers, IEEE 100, "The Authoritative Dictionary of IEEE Standards Terms," Piscataway, NJ.
2. Institute of Electrical & Electronics Engineers, IEEE Std 279-1968, "Proposed IEEE Criteria for Nuclear Power Plant Protection Systems," Piscataway, NJ.
3. Institute of Electrical & Electronics Engineers, IEEE Std 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations," Piscataway, NJ.
4. Institute of Electrical & Electronics Engineers, IEEE Std 379-2000, "IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems," Piscataway, NJ.
5. Institute of Electrical & Electronics Engineers, IEEE Std 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," Piscataway, NJ.
6. Institute of Electrical & Electronics Engineers, IEEE Std 603-1991, "Standard Criteria for Safety Systems for Nuclear Power Generating Stations," Correction Sheet, January 30, 1995.
7. U.S. Nuclear Regulatory Commission, "Manual Initiation of Protective Actions," Regulatory Guide 1.62, Revision 1, June 2010
8. U.S. Nuclear Regulatory Commission, "A Defense-in-Depth and Diversity Assessment of the RESAR-414 Integrated Protection System," NUREG-0493, March 1979.
9. U.S. Nuclear Regulatory Commission, "Application of the Single-Failure Criterion to Safety Systems," Regulatory Guide 1.53.
10. U.S. Nuclear Regulatory Commission, "Control Systems," NUREG-0800, SRP Section 7.7.
11. U.S. Nuclear Regulatory Commission, "Diverse Instrumentation and Control Systems," NUREG 0800, SRP Section 7.8.
12. U.S. Nuclear Regulatory Commission, "Transient and Accident Analysis," NUREG 0800, SRP Section 15.0.
13. U.S. Nuclear Regulatory Commission, "Human Factors Engineering," NUREG 0800, SRP Section 18.0, Revision 3, December 2016
14. U.S. Nuclear Regulatory Commission, "Digital Computer Systems for Advanced Light-Water Reactors," SECY-91-292, September 16, 1991.

15. U.S. Nuclear Regulatory Commission, "Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems," NUREG/CR-7007, December 2008.
16. U.S. Nuclear Regulatory Commission, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems," NUREG/CR-6303, December 1994.
17. 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.
18. 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.
19. U.S. Nuclear Regulatory Commission, "Plan for Addressing Common Cause Failure in Digital Instrumentation and Controls," SECY-18-0090, September 12, 2018.
20. U.S. Nuclear Regulatory Commission, "Quality Assurance Guidance for ATWS Equipment That Is Not Safety-Related," Generic Letter 85-06, April 16, 1985.
21. U.S. Nuclear Regulatory Commission, "Clarification on Endorsement of Nuclear Energy Institute Guidance in Designing Digital Upgrades in Instrumentation and Control Systems," Regulatory Issue Summary 2002-22 Supplement 1, May 31, 2018.

---

**Paperwork Reduction Act Statement**

To be determined when this document is final.

**Public Protection Notification**

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

---



## **BTP Section 7-19**

### **Description of Changes**

#### **GUIDANCE FOR EVALUATION OF DEFENSE IN DEPTH AND DIVERSITY TO ADDRESS COMMON CAUSE FAILURE IN DIGITAL SAFETY SYSTEMS**

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

The main purpose of this update is to provide clarification on sections of the guidance that proved challenging to implement based upon feedback received by internal and external stakeholders. This update improves readability and the flow of information such that it is clear to the reader that there is an established process for analyzing potential vulnerabilities to common-cause failures resulting from improper implementation of digital technology, in particular within software or software-based logic. This update clarifies the scope of applicability for all users and clearly states the applicability of this guidance to the change process in Title 10 of the *Code of Federal Regulations* (10 CFR) 50.59, "Changes, tests and experiments." The update provides for a graded approach that clarifies the technical rigor and analysis appropriate for structures, systems, and components of differing safety significance so that an adequate demonstration of safety is consistently applied. This is in addition to clarifying specific areas of guidance such as diversity, testing, and the addition of the concept of defensive measures, as various means that can be employed to eliminate further consideration of potential common-cause failures.