NUREG--0800

U.S. NUCLEAR REGULATORY COMMISSION

STANDARD REVIEW PLAN

BRANCH TECHNICAL POSITION 7--19

GUIDANCE FOR EVALUATION OF ~~DIVERSITY AND DEFENSE-IN-DEPTH~~COMMON CAUSE FAILURE HAZARDS DUE TO LATENT SOFTWARE DEFECTS IN DIGITAL ~~COMPUTER-BASED~~ INSTRUMENTATION AND CONTROL SYSTEMS

REVIEW RESPONSIBILITIES

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

Secondary – Organization responsible for the review of reactor systems and the organization responsible for the review of human factors engineering (HFE)

Review Note: The revision numbers of ~~Regulatory Guides (RG~~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

Revision 7 – August 2016

USNRC STANDARD REVIEW PLAN

This Standard Review Plan (SRP), NUREG 0800, has been prepared to establish criteria that the U.S. Nuclear Regulatory Commission (NRC) staff responsible for the review of applications to construct and operate nuclear power plants intends to use in evaluating whether an applicant/licensee meets the NRC regulations. The SRP is not a substitute for the NRC 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 SRP sections are numbered in accordance with corresponding sections in Regulatory Guide (RG) 1.70, "Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants (LWR Edition)." Not all sections of RG 1.70 have a corresponding review plan section. The SRP sections applicable to a combined license application for a new light-water reactor (LWR) are based on RG 1.206, "Combined License Applications for Nuclear Power Plants (LWR Edition)."

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

Requests for single copies of SRP sections (which may be reproduced) should be made to the U.S. Nuclear Regulatory Commission, Washington, DC 20555, Attention: Reproduction and Distribution Services Section by fax to (301) 415 2289; or by email to DISTRIBUTION@nrc.gov. Electronic copies of this section are available through the NRC public Web site at http://www.nrc.gov/reading rm/doc collections/nuregs/staff/sr0800, or in the NRC Agencywide Documents Access and Management System (ADAMS), at http://www.nrc.gov/reading rm/adams.html under ADAMS Accession No. ML16019A344.

Reports for Nuclear 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). Therefore, the individual revision numbers of RGs (except RG 1.97) and years of endorsed industry standards are not shown in this BTP. References to industry standards incorporated by reference into regulationregulations (Institute of Electrical and Electronics Engineers (IEEE) Standard (Std) 279-1968, IEEE Std 279-1971, and IEEE Std 603--1991) and industry standards that are not endorsed by the agency do include the associated year in this BTP. See Table 7--1 to ensure that the appropriate RGs and endorsed industry standards are used for the review.

A. BACKGROUND

~~Digital instrumentation and control~~Common-cause failures (CCFs) have been identified as a type of hazard that digital I&C (DI&C) systems could be more susceptible to due to the ability to integrate design functions using DI&C technology and its inherent complexity compared to analog technologies. DI&C systems or components can be vulnerable to ~~common-cause failure (~~ a CCF~~) caused by~~ due to defects in hardware or to latent defects in the software ~~errors~~ or software~~-developed logic, which could defeat the redundancy achieved by hardware architecture.~~ -based logic. Latent defects in hardware, software, or system components within redundant portions (e.g., safety divisions[1]) of a safety-related system can be triggered by an event or condition and thus lead to a systematic fault. A CCF hazard[2] (e.g., loss of the capability to perform a safety function) can result from the occurrence of such a systematic fault during a design-basis event (DBE). This BTP is focused on addressing CCF hazards resulting from systematic faults caused by latent defects in the software or software-based logic. [3]

A CCF of a DI&C system or component can also initiate the operation of a safety-related function or other design functions without a valid demand or can result in erroneous system actions. These conditions are typically referred to as "spurious operations," but the term can be used interchangeably with the term "spurious actuation." For this BTP, the term "spurious operations" is used.

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

In NUREG-0493, "A Defense-in-Depth and Diversity Assessment of the RESAR-414 Integrated Protection System," issued March 1979, the U.S. Nuclear Regulatory Commission (NRC) staff documented a defense-in-depth and diversity ~~and defense-in-depth~~ (D3) ~~analysis~~assessment of a digital computer-based reactor protection system (RPS) in which defense against software CCF ~~(or simply CCF hereafter)~~, which resulted in loss of a safety function during a DBE, was based upon an approach using a specified degree of system separation between echelons of defense. The RESAR-414 RPS ~~consists~~consisted of the reactor trip system (RTS) and the engineered safety features (ESF) actuation system ~~(ESFAS).~~ Subsequently, in SECY-91-292, "Digital Computer Systems for Advanced Light-Water Reactors," dated September 16, 1991, the NRC staff ~~included discussion of~~ discussed its concerns about CCF hazards in digital systems used in nuclear power plants (NPPs).

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

~~On the basis of experience in detailed reviews, the NRC staff has established acceptance guidelines for D3 assessments as described in this branch technical position (BTP). Further guidance reflected herein was established through the efforts of the DI&C Task Working Group No. 2 on D3 with the development of DI&C-ISG-02, "Task Working Group No. 2: Diversity and Defense-in-Depth Issues Interim Staff Guidance," Revision 2. This interim staff guidance (ISG) was developed with extensive review of D3 issues including both internal review within the NRC and external input through public meetings with representatives from industry, vendors, and the general public.~~

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

In summary, while the NRC considers ~~(~~CCF hazards due to software~~) CCF~~ in ~~digital~~DI&C systems to be beyond design basis, ~~NPPs~~the application should ~~be~~ include an evaluation of CCF hazards due to software in DI&C systems and should verify that the plant is protected ~~against~~from the effects of ~~anticipated operational occurrences (AOOs)~~these CCF hazards. In addition, the application should include an evaluation of sources of this CCF hazard that can result in spurious operations, some of which may be considered within the design basis, as discussed later in this BTP.

Over the years, the NRC staff has approved applications with numerous design solutions, and in some cases, multiple design solutions for a single DI&C system, to address CCF hazards in DI&C systems. During these reviews, the NRC staff has observed that different solutions may be used to address CCF hazards, and ~~postulated accidents with a concurrent CCF in the digital protection system.~~that one standard solution may not be applicable to all DI&C systems. This BTP provides guidance for reviewing the design and analysis for addressing CCF hazards due to latent software defects in DI&C systems.

1. Regulatory Basis

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

- For NPPs with CPs issued before January 1, 1971, Title 10 of the *Code of Federal Regulations* (10 CFR) 50.55a(h), "Protection and Safety Systems," requires compliance with ~~Institute of Electrical & Electronics Engineers (~~the plant-specific licensing basis or IEEE~~) Standard (~~ Std~~)~~ 603-1991 and the correction sheet dated January 30, 1995.

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

- For applications for construction permits (CPs), operating licenses (OLs), combined licenses (COLs), standard design approvals (SDAs), design certifications (DCs), filed after May 13, 1999, 10 CFR 50.55a(h) requires compliance with IEEE Std 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," and the correction sheet dated January ~~30, 1995. For NPPs with construction permits (CPs) issued before January 1, 1971, the applicant may elect to comply instead with its plant-specific licensing basis. For NPPs with CPs issued between January 1, 1971, and May 13, 1999, the applicant may elect to comply instead with the requirements stated in IEEE Std 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations."~~ 30, 1995.

~~IEEE Std 603-1991, Clause 5.1, requires in part that "safety systems shall perform all safety functions required for a design basis event (DBE) in the presence of any single detectable failure within the safety systems concurrent with all identifiable, but non-detectable failures."~~

~~IEEE Std 603-1991, Clause 6.2, "Manual Control," requires in part that means shall be provided in the control room to implement manual initiation at the division level of the automatically initiated protective actions.~~

~~IEEE Std 603-1991, Clause 7.2, "Manual Control," requires in part that the means of any manual control of any execute features shall not defeat requirements of Clauses 5.1 and 6.2.~~

~~IEEE Std 279-1971, Clause 4.2, requires in part that "any single failure within the protection system shall not prevent proper protective action at the system level when required."~~

~~IEEE Std 279-1971, Clause 4.17, "Manual Initiation," requires in part that the protection system shall include means for manual initiation of each protective action at the system level.~~

~~10 CFR 50.62, "Requirements for Reduction of Risk from Anticipated Transients without Scram (ATWS) Events for Light-Water-Cooled Nuclear Power Plants," requires in part various diverse methods of responding to ATWS.~~

~~10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities," Appendix A, "General Design Criteria for Nuclear Power Plants," General Design Criterion (GDC) 21, "Protection System Reliability and Testability," requires in part that "redundancy and independence designed into the protection system shall be sufficient to assure that (1) no single failure results in the loss of the protection function."~~

~~GDC~~

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

- GDC 22, "Protection System Independence," requires, in part, that the protection system design shall ensure "that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not

result in loss of the protection function. … Design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protection function." GDC 22 provides the regulatory basis for the requirement to address CCF hazards and for requiring the use of design techniques, such as functional diversity or diversity in component design, to prevent the loss of the protection function.

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

GDC 29, "Protection against Anticipated Operational Occurrences," requires, in part, defense against anticipated operational transients "to assure an extremely high probability of accomplishing safety functions."

- 10 CFR Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants," governs the issuance of applications for early site permits (ESPs), standard, DCs, combined licenses (COLs), standard design approvals (, 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 prior to January 10, 1997 that have, 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 hazards concurrent with a DBE.

- 10~~-~~ CFR~~-~~ 50.67 provides guideline values for fission product releases from currently operating NPPs ~~that have~~for which the licensee has implemented an alternative source term.

- 10~~-~~ CFR~~-~~ 50.34(a)(1)(ii)(D) provides site dose guideline values for CP ~~applicants and NPPs licensed to operate~~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 ~~DCs~~DC applications.

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

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

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

2. Relevant Guidance

~~RG 1.53, "Application of the Single-Failure Criterion to Safety Systems," clarifies the application of the single-failure criterion (GDC 21) and endorses IEEE Std 379, "IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems," providing supplements and an interpretation.~~

~~IEEE Std 379, Clause 5.5, establishes the relationship between CCF and single failures by defining criteria for CCF's that are not subject to single-failure analysis. This clause also identifies D3 as a technique for addressing CCF.~~

~~RG 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," which endorses IEEE Std 7-4.3.2, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," with a few noted exceptions, provides guidance for complying with requirements for safety systems that use digital computers. Additional guidance on the application of IEEE Std 7-4.3.2 is provided in SRP, Chapter 7, Appendix 7.1-D.~~

~~RG 1.62, "Manual Initiation of Protective Actions," includes information on diverse manual initiation of protective action.~~

- NUREG/CR~~-~~6303, "Method for Performing Diversity and Defense~~-~~in~~-~~Depth Analyses

of Reactor Protection Systems," issued December 1994, summarizes several D3 analyses performed after 1990 and presents a method for performing such analyses. Within NUREG/CR-6303, an analysis method is presented that postulates common-mode failures[4] that could occur within digital RPSs and determines what portions of a design need to implement additional D3 measures to address such failures.

- ~~The SRM on SECY-93-087~~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 hazard. NUREG/CR-7007 identifies and develops a baseline set of diversity criteria that may constitute appropriate mitigating diversity strategies to address potential vulnerabilities to CCF hazards. 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 the SRM on SECY-93-087, Item 18, describes the NRC position ~~on D3 in Item 18, II.Q.~~ concerning mitigation of potential common mode failures.

- SECY-18-0090 provides the NRC staff's plan to clarify the guidance associated with evaluating and addressing CCF hazards of DI&C systems.

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

~~NUREG-0800, SRP Chapter 18, Appendix 18-A, "Crediting Manual Operator Actions in Diversity and Defense-in-Depth (D3) Analyses," defines a methodology, applicable to both existing and new reactors, for evaluating manual operator actions as a diverse means of coping with AOOs~~

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

~~and postulated accidents that are concurrent with a software CCF of the DI&C protection system.~~

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

- NUREG~~-~~-0800, SRP Section~~-~~ 7.8, "Diverse Instrumentation and Control Systems," describes the review process and additional acceptance criteria for diverse I&C systems provided to protect against CCF hazards.

- 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 anticipated operational occurrences (AOOs) and postulated accidents that are concurrent with a CCF hazard due to latent defects that disables a safety function credited in the safety analysis report (SAR).

3. Scope

The guidance of this BTP is intended for reviews of (1) proposed modifications that require a license amendment to be implemented, and (2) applications for CPs, OLs, COLs, DCs, SDAs, and MLs. This BTP is not applicable to proposed modifications performed under the 10 CFR 50.59, "Changes, Tests and Experiments," change process.

~~3.~~4. Purpose

The purpose of this BTP is to provide guidance for ~~evaluating~~reviewing an evaluation of (1) a DI&C system's vulnerability to a CCF hazard due to latent defects in the software or software-based logic, (2) any diverse means credited to address remaining vulnerabilities to a CCF hazard, and (3) the effects of any unmitigated vulnerabilities to a CCF hazard on plant safety. This BTP also provides guidance on implementing a graded approach to address CCF hazards due to latent defects in the software or software-based logic in DI&C systems based on the safety significance of the system. In this guidance, software includes software, firmware,[5] and logic developed from software-based development systems (e.g., hardware description

[5] 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.

language programmed devices).

This BTP is intended to address an applicant's ~~D3 assessment,~~ approach to address CCF hazards caused by latent defects in the software or software-based logic. This type of CCF hazard is considered a beyond-design~~, and the~~ basis event for structures, systems, and components (SSCs) that employ a robust design ~~of~~process to reduce the likelihood of design defects. The plant response to these beyond-design-basis events may be analyzed using either conservative or best-estimate methods. However, in integrated DI&C systems, a single random hardware failure can have cascading effects, similar to a CCF hazard (e.g., loss of multiple functions within a safety group, or spurious operation of functions within multiple safety groups). Single random hardware failures with cascading effects are considered DBEs, because random hardware failures are expected during the life of the facility. DBEs should be analyzed using conservative methods to demonstrate that the plant response to these events is bounded by the events in the accident analysis section of the SAR. RG 1.53 provides guidance for the deterministic analysis of single failures in safety-related systems.

This BTP provides guidance for reviewing (1) design attributes, such as the use of diverse equipment within a system or component to eliminate the CCF hazard from further consideration,[6] (2) diverse external equipment, including manual controls and displays to mitigate a CCF hazard, and (3) other measures to ensure conformance with the ~~NRC~~NRC's position on ~~D3 for I&C systems incorporating digital, software-based or software-logic-based RTS or ESF, auxiliary supporting features, and other auxiliary features as appropriate. This BTP has the objective of confirming that vulnerabilities to CCF have been addressed in accordance with the guidance of the SRM on SECY-93-087 and clarification provided in this staff guidance, specifically~~addressing CCF hazards in DI&C systems as specified in the SRM on SECY-93-087 and SECY-18-0090. The objectives of this review are to verify the following:

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

- For DI&C systems of high safety significance, an adequate ~~diversity~~D3 assessment has been ~~provided in a design to~~ conducted and meets the acceptance criteria described in this BTP. An adequate D3 assessment consists of
  - An evaluation of vulnerabilities to a CCF hazard due to latent defects in system and the effectiveness of any credited attributes to eliminate the CCF hazard from further consideration;
  - Identification of any credited diverse means to mitigate CCF hazards that have not been eliminated from further consideration and the evaluation of the effectiveness of these diverse means; and

[6] The description of how a CCF hazard is eliminated from further consideration is discussed in Section B.3.1 of this BTP.

- An assessment of the consequences of residual CCF hazards that have not been eliminated from further consideration or mitigated to demonstrate that the consequences remain bounded[7] by the events analyzed in the accident analyses.

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

- ~~Verify that adequate defense-in-depth has been provided in a design to meet the criteria established by NRC guidance.~~

- ~~Verify that the displays and manual controls for plant critical safety functions initiated by operator action are diverse from digital systems used in the automatic portion of the protection systems.~~

This BTP also addresses the applicant's assessment of vulnerabilities to a CCF hazard due to latent software defects that can cause the spurious operation of a safety-related component or a component that is NSR, because 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. This BTP provides criteria for reviewing an applicant's assessment of CCF hazards of DI&C systems that can result in spurious operation of safety-related components or components that are NSR.

B. BRANCH TECHNICAL POSITION

~~1.0~~1. Introduction

~~1.1. Echelons of Defense~~

~~The NRC staff identified four echelons of defense in NUREG/CR-6303:~~

- ~~Control System - The control system echelon usually consists of equipment that is not safety-related that is used in the normal operation of a 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~~

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

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.

1.1. 1.2 Plant Four Common-Cause Failure Positions and Clarification

1.1. Critical Safety Functions

As described in NUREG-0737, "Supplement No. 1, Clarification of TMI Action Plan Requirements," sufficient information should be provided to the nuclear reactor operators to monitor (and thereby control) the following plant critical safety functions and conditions:

1. Reactivity control
2. Reactor core cooling and heat removal from the primary system
3. Reactor coolant system (RCS) integrity
4. Radioactivity control
5. Containment conditions

1.3 Combining RTS and ESFAS

In addition to divisional independence, many earlier analog I&C architectures consisted of discrete and separate analog components in each echelon of defense. In digital systems, formerly discrete systems (e.g., the RTS and the ESFAS) could be combined into a single DI&C system. Digital systems that combine most, if not all, RTS and ESFAS functions within a single digital system using a limited number of digital components in both new NPP designs and upgrades to current operating plant systems could introduce new effects from single failures as well as CCF effects that do not exist in systems that use separate discrete components. While a single random failure could affect multiple echelons in one division, a CCF could affect multiple echelons in multiple divisions. However, the four echelons of defense described above are only conceptual and, with the exception of the monitoring and indication echelon of defense noted in Point 4 (see Section B.1.4, "Four-Point Position,") NRC regulations do not require nor does this guidance imply that RTS and ESFAS echelons of defense must be independent or diverse from each other with respect to a CCF. Plant responses to postulated CCF that could impair a safety function should be in accordance with the acceptance criteria of this BTP, regardless of the echelons of defense that may be affected.

1.4 Four-Point Position

On the basis of reviews of the ALWR DC applications for designs that use digital safety systems, the NRC has established the following four-point position on D3 for new reactor designs and for digital system modifications to operating plants. The foundation of BTP 7-19 is

the "NRC position on D3" from the SRM on SECY-93-087, Item 18, II.Q. The four points (i.e., positions stated in the SRM on SECY-93-087 items) are quoted below:

Point 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."

Point 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).

Point 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 nonsafetynon-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions." (emphasis in original).

Point 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 on SECY-93-087, Item 18, a D3 assessment should be performed. Section B.3 of this BTP provides review guidance and acceptance criteria for a D3 assessment to demonstrate that vulnerabilities to CCF hazards have been adequately addressed. The guiding principles 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 that is necessary to address CCF hazards. This graded approach is described in Section B.2.1 of this BTP.

The term "best-estimate methods" in Point Position 2 is more accuratelynow referred to as methods using "realistic assumptions," which are defined as normalthe initial plant conditions corresponding to the onset of the event. For example being analyzed. Initial plant event conditions include the following:

- power levels,
- temperatures,
- pressures,

- flows~~, and~~
- 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, ~~in~~when performing the ~~assessment, the vendor or applicant should analyze each postulated CCF for each event that is evaluated in the SAR section analyzing power operation accidents at the plant conditions corresponding to the event. This analysis may use~~D3 assessment, it is acceptable to use either realistic assumptions to analyze the plant response to DBEs, or the conservative assumptions on which the ~~Chapter 15, SAR analysis is based~~accident analysis 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 analysis indicates a postulated CCF could disable a safety function, then Point 3 directs that an applicant should identify an existing diverse means or add a diverse means that may be nonsafety (see Section 1.6, "D3 Assessment"). Point 3 also addresses manual initiation methods of RTS and ESFAS, if subject to a postulated CCF.~~

If the D3 assessment shows a postulated CCF could disable a safety function (i.e., become a CCF hazard), 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 unlikely to be subject to the same CCF hazard. While the enclosure to Generic Letter 85-06 provides quality assurance guidance for ATWS equipment, this guidance can also be applied to equipment that is NSR credited as the diverse means for addressing CCF hazards. 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 CCF hazard, when evaluated in the accident analysis can be reasonably mitigated through other means (such as with current 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 CCF hazard 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 pursuant to 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 systems that are NSR should be met.

Position

~~The independence requirements of a diverse protection system from the safety protection system (i.e., physical, electrical, and communication separation) are defined in IEEE Std 603-1991. The diverse means could be safety-related and part of a safety division, and would then be subject to meeting divisional independence requirements. The diverse means could also be nonsafety-related in which case the IEEE Std 603-1991 requirement to separate safety-related equipment from that which is not safety-related would still apply and would require independence of the two systems. In either case, the diverse means should be independent of the safety system such that a CCF of the safety system would not affect the diverse system.~~

~~Point~~ 4 directs the inclusion of a set of displays and manual controls ~~(~~("safety" or ~~nonsafety)~~"non-safety") in the main control room (MCR) that is diverse from any ~~CCF~~ vulnerability to a CCF hazard identified within the "safety computer system" discussed in ~~Points~~ Positions 1 and 3 above and meets divisional independence requirements as applicable for the specific design implementation. ~~These~~ While the SRM on SECY-93-087 uses the terms "safety" and "non-safety," these terms in context refer to safety-related and NSR SSCs, respectively. Depending on the design, these displays and controls ~~are for~~should provide manual~~,~~ system~~-level~~ or divisional level ~~(depending on the design)~~ actuation and control of equipment to manage the ~~"(plant)~~ "critical safety functions" (see Section B.1.2 ~~above~~). Further, if not subject to the ~~CCF~~same CCF as the proposed safety-related DI&C system, some of these displays and manual controls from ~~Point~~ Position 4[8] may ~~actually~~ be credited as all or part of the diverse means ~~called for under Point 3.~~provided to address Position 3.

The ~~Point~~ Position 4 phrase ~~". . ."~~"safety computer system identified in Items 1 and 3 above" refers to ~~the safety-related automated RTS and ESFAS.~~a safety-related DI&C system that is credited for mitigating an AOO or postulated accident 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.

~~For digital system modifications to operating plants, retention of existing analog displays and controls in the MCR could satisfy this point (see Section B.1.5, "Manual Initiation of Automatically Initiated Protective Actions Subject to CCF.") However, if existing displays and controls are digital and/or the same platform is used to provide signals to the analog displays, this point may not be satisfied.~~

~~Where the Point 4 displays and controls serve as the diverse means, the displays and controls also should be able to function downstream of the lowest-level components subject to the CCF that necessitated the use of the diverse means. One example would be the use of hard-wired connections.~~

The four positions

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

~~Once~~ ~~manual actuation~~ from the ~~MCR using the Point 4 displays and controls has been completed, controls outside the MCR for long-term management of these (plant) critical safety functions may be used when supported by suitable HFE analysis and site-specific procedures or instructions.~~

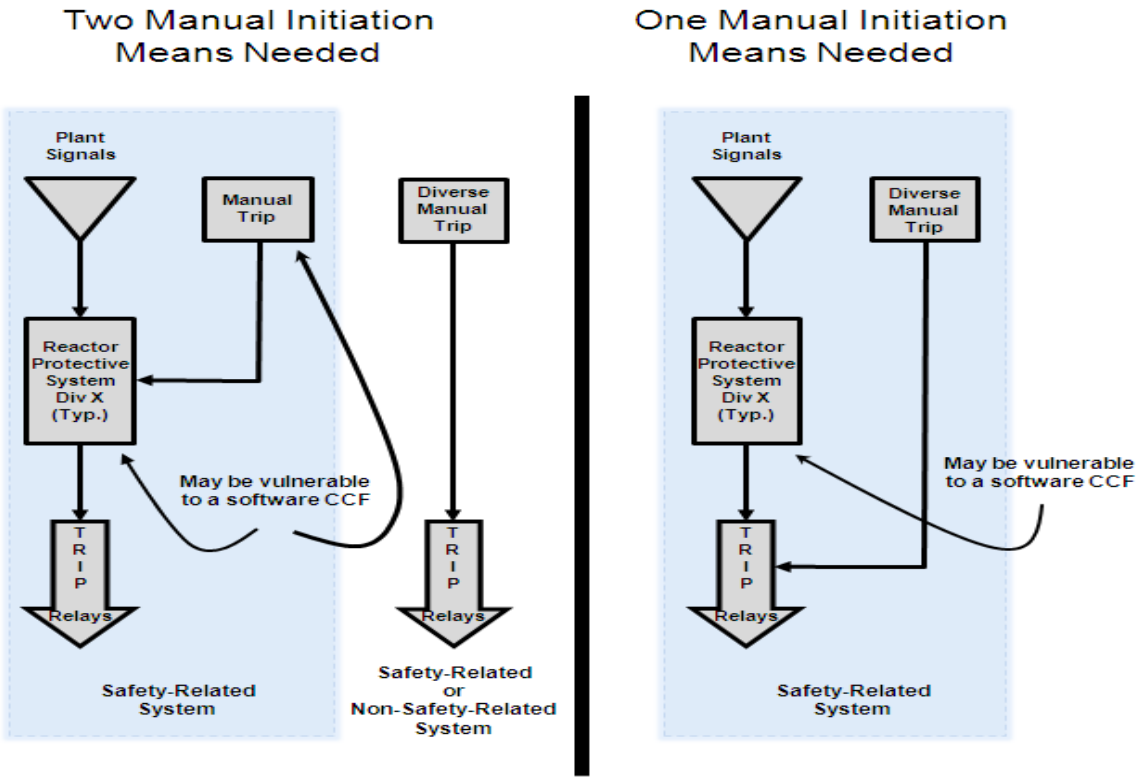
~~The above four-point position is based~~ SRM on ~~the NRC concern~~SECY-93-087, acknowledge that ~~software based or software logic based digital~~DI&C system development errors (i.e., latent defects) are a credible source of CCF~~. In this guidance, common software includes software, firmware,[9] and logic developed from software-based development systems.~~ hazards. Generally, ~~digital~~DI&C systems containing software or logic cannot be ~~proven to be error-free and, therefore, are considered susceptible to CCF~~ fully tested except for very limited cases, nor can their failure modes be completely predicted because software does not have a physical manifestation that limits its behavior. Therefore, DI&C systems may be vulnerable to CCF hazards if either (1) identical system designs and identical copies of the software or software-based logic ~~and architecture~~ are present in redundant divisions of safety-related systems~~.~~, or (2) previously separated functions have been integrated into a single DI&C system. Also, some errors, such as those labeled as "software design errors~~" (for example) actually~~," normally result from errors in the higher-level requirements (e.g., system requirements or design specifications ~~used to direct~~), in which the system ~~development that fail in some way to represent~~design misrepresents the actual process. ~~Such errors place further emphasis on the need for diversity to avoid or mitigate CCF.~~

~~1.5 Manual Initiation of Automatically Initiated Protective Actions Subject to CCF~~

~~Two types of manual initiation of automatically initiated protective actions may be necessary. To satisfy IEEE Std 603-1991 Clauses 6.2 and 7.2, a safety-related means shall be provided in the control room to implement manual initiation of the automatically initiated protective actions at the division level. System level actuation of all divisions also may be used to meet the requirements of IEEE Std 603-1991.~~

~~If a D3 analysis indicates that the safety-related manual initiation would be subject to the same potential CCF affecting the automatically initiated protective action, then under Point 3 of the NRC position on D3, a diverse manual means of initiating protective action(s) would be needed (i.e., two manual initiation means would be needed). This diverse manual means may be safety or nonsafety. If the system/division level manual initiation required by IEEE Std 603-1991 is sufficiently diverse, the diverse (second) manual system level or division level actuation would not be necessary for the automated protective actions (see Figure 1).~~

~~[9] IEEE 100, "The Authoritative Dictionary of IEEE Standards Terms," defines firmware as the combination of a hardware device and computer instructions and data that reside as read-only software on that device.~~



~~Figure 1. Two Manual Initiation Methods verses One Initiation Method~~

~~1.6 D3 Assessment~~

~~To defend against potential CCF, the NRC staff considers D3 and the use of defensive measures to avoid or tolerate faults and to cope with unanticipated conditions to be key elements in high quality digital system designs. However, despite high quality in the development and use of defensive design measures, system errors could still defeat safety functions in redundant, safety-related channels. Therefore, as set forth in Points 1, 2, and 3 of the NRC position on D3, the applicant should perform a D3 assessment of the proposed DI&C system to demonstrate that vulnerabilities to CCF have been adequately addressed. In this assessment, the applicant may use realistic assumptions to analyze the plant response to DBEs (as identified in the SAR). If a postulated CCF could disable a safety function that is credited in the safety analysis to respond to the DBE being analyzed, a diverse means of effective response (with documented basis) is necessary. The D3 analysis methods used in ALWR DC applications and for operating plant upgrades are documented in NUREG/CR-6303, which describes an acceptable method for performing such assessments.~~

As used in this BTP, terms

~~When~~ ~~the RTS and ATWS mitigation system in an operating plant is modified, the requirements~~

~~of the ATWS rule, 10 CFR 50.62, must be met. 10 CFR 50.62 requires that the ATWS mitigation system be composed of equipment that is diverse from the RTS. If "sufficient" diversity in manufacturer cannot be demonstrated, a case-by-case assessment of the mitigation system designs should be conducted. This assessment should include differences~~ such as ~~manufacturing division (within a corporate entity), software (including implementation language), equipment (including control processing unit architecture), function, and people (design and verification/validation team).~~

~~1.7 The Diverse Means~~

~~When a diverse means is needed to be available to replace an automated system used to~~ "higher-level requirements" do not refer to NRC regulatory requirements but to system or component design or operating characteristics that are relied upon to accomplish ~~a credited safety function as a result of the D3 assessment identifying a potential CCF, the credited safety function (or a different function that will accomplish the same desired safety protection) can be accomplished via either an automated system or manual operator actions performed from the MCR. The preferred diverse means is generally an automated system.~~

~~The primary focus of BTP 7-19 is to identify~~ the stated system or component functions. Throughout this BTP, context indicates whether ~~a diverse means of performing protective actions is necessary due to an automated safety function being subject to a postulated CCF. Functions performed manually normally would be expected to still be performed manually in the presence of a CCF (even if different equipment is called upon to function). If the manual actuation method could be adversely affected by the postulated CCF, then a diverse manual means is needed to perform the safety function or an acceptable different function.~~requirements are NRC regulatory requirements.

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

- Identified vulnerabilities to CCFs due to a design or implementation defect in a DI&C system and evaluated the impacts of these postulated CCFs to safety functions or other design functions to determine whether these postulated CCFs can lead to a hazard;
- Demonstrated that a CCF hazard due to these residual defects has been either adequately prevented through use of appropriate measures (e.g., diversity within the design, testing, and defensive measures) or mitigated through use of a diverse means; and
- Assessed the ability of the overall plant design (e.g., I&C systems, mechanical systems, and manual operator action) to maintain plant safety, using conservative or "best

estimate" methods, for those CCF hazards that have not been shown to be prevented or mitigated.

1.2. Critical Safety Functions

~~1.8 Potential Effects of CCF: Failure to Actuate and Spurious Actuation~~

~~There are two inherent safety functions that safety-related trip and actuation systems provide. The first safety function is to provide a trip or system actuation when plant conditions necessitate that trip or actuation. However, in order to avoid challenges to the safety systems and to the plant, the second function is to not trip or actuate when such a trip or actuation is not required by plant conditions.~~

~~A simple metric would be:~~

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

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

2.1. Graded Approach for Categorizing Digital Instrumentation and Control Systems

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

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

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

~~Trip or Actuation does not occur~~**Not Safety Significant** Not a significant contributor to plant safety	~~System Failure (Actuation does not occur or incomplete activation)~~**A2 DI&C SSCs** Provides an auxiliary or indirect function in the achievement or maintenance of plant safety. **or** Maintains the plant in a safe shutdown state after the plant has reached initial safe shutdown state.[10] **Application should include a qualitative assessment as described in Section B.4**	~~Proper System Operation~~**B2 DI&C SSCs** 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). **and** Failure does not have consequences to plant safety or whose failure can be detected and mitigated with significant safety margin. **Application may need to include a qualitative assessment as described in Section B.4** if the proposed design could introduce conditions[11] that have not been previously analyzed in the SAR.

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

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

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

System integration and interconnectivity among the categories identified in Table 2-1 can introduce additional vulnerabilities to CCF hazards. If there is integration (e.g., through combined design functions, shared resources, or digital interconnectivity) among A1 systems or among A1 and systems in the other three categories, then the assessment for the proposed A1 system should consider the CCF hazards of the integrated system and the consequences of these CCF hazards that could affect the integrated or interconnected A1 systems. For example,

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

if a digital protection system includes controllers for performing reactor trip and ESF logic as well as safety-related control functions (e.g., auxiliary feedwater level control), and the reactor trip or ESF initiation signal only reaches the final actuation device via the equipment that performs these safety-related control functions, then the categorization of all the equipment in that pathway should be 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. Diversity and Defense-in-Depth (D3) Assessment

A D3 assessment is necessary for a proposed A1 system or component to determine whether vulnerabilities to CCF hazards have been adequately addressed. For each event analyzed in the accident analysis section of the safety analysis report, the results of the D3 assessment should show that vulnerabilities to CCF hazards have been adequately addressed through any combination of the following:

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

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

c. The consequences of the CCF hazard are acceptable for the associated DBE per the acceptance criteria within Section B.3.3.

The applicant may elect to apply any combination of the above three methods to the entire A1 system or portions of the A1 system. For example, the applicant may show that the CCF hazard has been eliminated for a component within the A1 system and exclude this component when addressing the CCF hazard for the rest of the A1 system.

The adequacy of the ~~A failure of a system to actuate might not be the worst case failure, particularly when analyzing the time required for identifying and responding to conditions resulting from a CCF 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 cases such as this, 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. For this reason, the evaluation of failure modes as a result of CCF should include the possibility of partial 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. The primary concern is that an undetected failure within a digital safety system could prevent proper system operation. A failure or fault that is detected can be addressed; however, failures that are non-detectable may prevent a system actuation that is necessary. Consequently, non-detectable faults are of concern. Therefore, a diverse means to provide the credited safety function or some other~~

~~safety function that will adequately address each DBE should be provided.~~

~~A CCF that causes an undesired trip or actuation 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.~~

~~Failures of the automated protection system stemming from a software CCF can cause spurious actuations. The plant design basis addresses the effects of certain software CCF-caused spurious actuations.~~

~~The overall defense in depth strategy of a plant should prevent or mitigate the effects of credible spurious actuations caused by a software CCF that have the potential to place a plant in a configuration that is not bounded by the plant's design basis. The effects of some credible postulated spurious actuations caused by a software CCF in the automated protection system may not be evaluated in design basis accident analyses. In these cases, an analysis should be performed to determine whether these postulated spurious actuations could result in a plant response that results in conditions that do not fall within those established as bounding for plant design. Further, the analysis should identify whether adequate coping strategies, whether for prevention or mitigation, exist for these postulated spurious actuations (e.g., emergency, normal, and diverse equipment and systems, controls, displays, procedures and the reactor operations team). If existing coping strategies are not effective for responding to the credible postulated spurious actuations that result in plant conditions falling outside those established as bounding for plant design, the licensee should develop additional coping strategies.~~

~~1.9 Design Attributes~~D3 assessment, including any (1) measures used to eliminate the CCF hazard from further consideration, (2) diverse means provided to mitigate the CCF hazard, or (3) analysis to show the consequences of the CCF hazard are acceptable for each DBE, should be justified in the application and explicitly addressed in the NRC staff's safety evaluation.

3.1. Means to Eliminate Common-Cause Failure Hazard from Further Consideration ~~of CCF~~

Many system design and testing attributes, procedures, measures, and practices can contribute to significantly reducing the ~~probability~~likelihood of a CCF hazard. However, there are ~~two~~certain design attributes~~, either of which is~~ that are sufficient to eliminate from further consideration ~~of software based or software logic based~~ a CCF~~:~~

~~Diversity or Testability~~

~~(1) Diversity – If sufficient diversity exists in the protection system, then the potential for CCF within the channels can be considered~~ hazard due to ~~be appropriately~~

~~addressed without further action.~~

~~Example: An RPS design in which each safety function is implemented in two channels that use one type of digital system and another two channels that use a diverse digital system. If a D3 analysis performed consistent with the guidance in NUREG/CR-6303 determines that the two diverse~~ digital ~~systems are not subject to a CCF, then, in this case, no additional diversity would be necessary in the safety system.~~

~~(2) Testability – A system is sufficiently simple such that every possible combination of inputs and every possible sequence of device states are tested and all outputs are verified for every case (100 percent tested).~~

~~What constitutes "sufficient diversity" should be evaluated on a case-by-case basis, considering diversity~~design or implementation defect. These attributes ~~and attribute criteria that preclude or limit certain types of CCF. Diversity~~include (1) diversity within the DI&C system or component, (2) testability, and (3) defensive measures within the design. Although these attributes ~~and associated attribute criteria, and a process for evaluating the application may provide more objective guidance in answering, "What is sufficient diversity?"~~do not eliminate the CCF hazard completely, the residual risk for a CCF hazard is minimized such that no further evaluation is necessary. The basis for the acceptability of this residual risk is discussed for each attribute in the subsections below.

~~2. Information to be Reviewed~~

If the application demonstrates that use of these attributes for an A1 system or component meet the criteria within this BTP, then the CCF hazard has been eliminated from further consideration. Thus, separate diverse means do not need to be provided, and an analysis of the plant's response for each AOO or postulated accident concurrent with a CCF of the proposed A1 system does not need to be performed for the portion of the A1 system or component that credit these attributes.

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

If sufficient diversity exists within each safety division or among redundant safety divisions of an A1 system to perform the safety function, then the CCF hazard can be eliminated from further consideration. 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. In this case, the application should include 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 hazard such that further consideration is unnecessary. Given that this analysis is qualitative in nature, the potential that a CCF hazard can affect both diverse divisions is minimized but not eliminated. However, the

potential of a CCF hazard due to latent defects in the software of the diverse portions is much lower than failures that are considered in the accident analysis (e.g., single failures) and comparable to other CCF hazards that are not considered in the accident analysis (e.g., design flaws, maintenance errors, calibration errors).

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

~~The information to be reviewed is the D3 assessment conducted by the applicant. If the D3 assessment indicates the need for a diverse means to accomplish a protective safety function, then the diverse means should be evaluated, including any HFE analysis associated with manual operator actions as a diverse means.~~

~~3.~~ Acceptance Criteria

~~3.1 Specific Acceptance Criteria~~

The ~~D3 assessment submitted by the applicant~~reviewer should ~~demonstrate compliance with the NRC position on D3 described above. To~~ reach a conclusion ~~of acceptability,~~that the application provides adequate information on the use of diversity within the A1 system or component to eliminate CCF hazards from further consideration, if the application demonstrates the following ~~conclusions should be reached and supported by summation of the results of the analyses and the diverse means provided. Since the~~ acceptance criteria ~~address confirmation that AOOs and postulated accidents~~ are ~~mitigated in the presence of CCF, the focus of the D3 analyses should be on the protection systems. Other systems important to~~ met:

a. Each safety ~~become involved only~~ function to ~~the extent that they are credited as providing~~ 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 A1 system or component in accordance with the guidance of NUREG/CR-6303 and NUREG/CR-7007.

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 A1 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 Common-Cause Failure Hazard from Further Consideration

When ~~to protect against~~considering CCF ~~in the protection systems.~~hazards in DI&C systems or components, there are two general areas of concern: (1) CCF hazards as a result of errors introduced by the system or software requirements, and (2) CCF hazards as a result of errors introduced during the design and implementation of the software or software-based logic. A quality development process can be credited to address potential errors in the system or component requirements or specifications for both analog and digital equipment. However, the quality of the development process cannot eliminate potential defects introduced during the design and implementation process. Testing can identify latent defects that could lead to a CCF hazard in the design, fabrication, and implementation of software or software-based logic. Testing can be used to both identify latent defects for correction in the design, fabrication, and implementation process and to demonstrate that any potential latent defects have been corrected.

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

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

a. The combination of every possible input. Any unused inputs to the component that will be permanently forced to a fixed state can be set at that fixed state. The design does

not include any analog input.

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

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

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

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

Acceptance Criteria

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

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

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

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

d. Any application that excludes from the test cases logic or circuits of devices or components, because they are not used under any operational condition, has demonstrated that the logic or circuits excluded do not interfere with the proper operation of the device regardless of (1) any possible malfunction or failure within the device, (2) any condition external to the device, or (3) any aspect of the operation of any other

logic or circuits included in the device.

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

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

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

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

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

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

e. an assessment of any residual risks from CCF hazards

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

Acceptance Criteria

The reviewer should reach a conclusion that the application provides sufficient information on the credited defensive measures to eliminate a CCF hazard 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 a technical basis and acceptance criteria are submitted in the application, the NRC staff will review the information on a case-by-case basis.

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

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

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

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

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

   1. whether the safety function is needed,

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

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

3.2.1. Crediting Existing Systems

An existing highly 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 postulated accident in the safety analysis report. An analysis should be performed to demonstrate that the existing plant system to be credited and the digital design used for the proposed A1 system are not subject to the same postulated CCF. Section 2.6 of NUREG/CR-6303 identifies six diversity attributes and 25 related diversity criteria that can be used to support this qualitative analysis. NUREG/CR-7007 identifies and develops a baseline set of diversity criteria that may constitute appropriate mitigating diversity strategies to address vulnerabilities to CCF hazards.

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. For existing systems that are NSR, the quality of these systems should be similar to systems required by the ATWS rule (i.e., 10 CFR 50.62), as described in the enclosure to Generic Letter 85-06. For example, plant ATWS design capabilities may be credited as a diverse means of achieving reactor shutdown, provided that the ATWS system design to be credited is capable of responding to the same analyzed events as the proposed A1 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 postulated accident sequences using independent sensors and actuators as the proposed DI&C system.

Acceptance Criteria

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

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 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 these options, the application should show that the capabilities for sensing and responding maintain plant safety by verifying plant conditions stay within the acceptance criteria specified for each AOO or postulated accident in the safety analysis report.

3.2.2. Crediting Manual Operator Action

Manual operator action that can be performed within an acceptable time frame, as defined in SRP Chapter 18, can be used as a diverse means to provide the same or a different function credited in the D3 assessment. If manual operator action is used as the diverse means, the equipment necessary to perform such action, including the supporting indications, should be diverse and independent from the safety-related I&C system disabled by a postulated CCF. 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 sufficient quality. This equipment should be similar in quality to that required by the ATWS rule (i.e., 10 CFR 50.62), as described in the enclosure to Generic Letter 85-06. Functional characteristics (e.g., range, accuracy, time response) should be sufficient to provide operators with the information needed to place and maintain a plant in a safe ~~occurrence~~ shutdown condition. A CCF hazard that affects normal displays or controls should not prevent the operator from manually performing the safety functions.

The application should contain an HFE analysis in accordance with the guidance of SRP Chapter 18, to demonstrate that plant conditions can be maintained within specified acceptance criteria for the particular AOO or postulated accident. The credited manual operator action and the equipment necessary to perform the action should be identified. If equipment outside of the MCR 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 should be applied to the selection and design of the displays and controls. Human-performance requirements should be described and related to the plant safety criteria. Recognized human-factors standards and design techniques should be employed to support the described human-performance requirements.

Acceptance Criteria

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

a. The manual operator action can be performed within an acceptable time frame as specified in SRP Chapter 18. The difference between the time available to perform the operator action, as determined by the thermal-hydraulic analysis, and the time necessary to perform it, as determined by the HFE analysis, is a measure of the safety margin. As this margin decreases, the uncertainty in the estimate of the difference between these times should be appropriately considered. This uncertainty could reduce the level of assurance and potentially invalidate a conclusion that operators can reliably perform the action within the time available. For complex situations and for manual operator action with limited margin between time available and time necessary, a more focused staff review will be performed.

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

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

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

3.2.3. Crediting a Diverse System

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

six diversity attributes and 25 related diversity criteria that can be used to support this qualitative analysis.

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

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

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

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

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

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

Acceptance Criteria

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

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

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

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

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

consequences to plant safety. The basis for the priority ranking should be documented.

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

3.3. Consequences of the CCF Hazard Are Acceptable

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

Acceptance Criteria

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

~~(1)~~a. For each AOO in the design basis occurring in conjunction with ~~each single postulated~~the CCF hazard, the plant response calculated using realistic or conservative assumptions ~~should~~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. ~~The applicant should: (1) demonstrate that sufficient diversity exists to achieve these goals, (2) identify the vulnerabilities discovered and the corrective actions taken, or (3) identify the vulnerabilities discovered and provide a documented basis that justifies taking no action.~~

~~(2)~~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 ~~should~~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). ~~The applicant should (1) demonstrate that sufficient diversity exists to achieve these goals, (2) identify the vulnerabilities discovered and the corrective actions taken, or (3) identify the vulnerabilities discovered and provide a documented basis that justifies taking no action.~~

~~c. When a failure of a common element or signal source shared by the control system and RTS is postulated and the CCF results in a plant response for which the safety analysis credits reactor trip but the failure also impairs the trip function, then diverse means that are not subject to or failed by the postulated failure should be provided to perform the RTS function. The diverse means should~~

assure that the plant response calculated using realistic assumptions and analyses 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.

d. When a CCF results in a plant response for which the safety analysis credits ESF actuation and also impairs the ESF function, then a diverse means not subject to or failed by the postulated failure should be provided to perform the ESF function. The diverse means should assure that the plant response calculated using realistic assumptions and analyses 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.

e. No failure of monitoring or display systems should influence the functioning of the RTS or ESF. If a plant monitoring system failure induces operators to attempt to operate the plant outside safety limits or in violation of the limiting conditions of operation, the analysis should demonstrate that such operator-induced transients will be compensated by protection system function.

f. For safety systems to satisfy IEEE Std 603-1991 Clauses 6.2 and 7.2, a safety-related means shall be provided in the control room to implement manual initiation of the automatically initiated protective actions at the system level or division level (depending on the design) of the RTS and ESF functions. This safety-related manual means shall minimize the number of discrete operator manual manipulations and shall depend on operation of a minimum of equipment. If a D3 analysis indicates that the safety-related manual initiation would be subject to the same potential CCF affecting the automatically initiated protective action, then under Point 3 of the NRC position on D3, a diverse manual means of initiating protective action(s) would be needed, (i.e., two manual initiation means would be needed). If the safety-related system/division level manual initiation required by IEEE Std 603-1991 is sufficiently diverse, the diverse (second) manual means would not be necessary (see Section B.1.5, "Manual Initiation of Automatically Initiated Protective Actions Subject to CCF.") If credit is taken for a manual actuation method that meets both the IEEE Std 603-1991, Clauses 6.2 and 7.2 requirements and a need for a diverse manual means, then the applicant should demonstrate that the criteria are satisfied and that sufficient diversity exists. Note that if the diverse means is nonsafety, then IEEE Std 603-1991, Clause 5.6, "Independence," directs the separation or independence of the safety systems and the diverse means (see Figure 1).

g. If the D3 assessment reveals a potential for a CCF, then the method for accomplishing the diverse means of actuating the protective safety functions can be achieved via either an automated system (see Section 3.4, "Use of

~~Automation in Diverse Means" below,) or manual operator actions that meet HFE acceptability criteria (see Section 3.5, "Use of Manual Action as a Diverse Means of Accomplishing Safety Functions" below).~~

4. Qualitative Assessment

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

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

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

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

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

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

Acceptance Criteria

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

The reviewer should reach a conclusion that the application has addressed a CCF hazard in A2, B1, or applicable B2 systems if the application provides a qualitative assessment demonstrating the likelihood of the CCF hazard is sufficiently low based on any of the following criteria :

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

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

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

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

5. Spurious Operation Assessment

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

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

Acceptance Criteria

The reviewer should reach a conclusion that the application includes adequate information on the results of the spurious operation assessment if the application demonstrates the spurious operation of safety-related components or components that are NSR assumed in the accident analysis have not been invalidated by the proposed modification of the DI&C system or component.

5.2. IEEE Std 603-1991 Applies

Pursuant to the incorporation by reference in 10 CFR 50.55a, IEEE Std 603-1991, Clauses 4.8 and 5.6.3, require that safety-related systems be designed to prevent conditions that can lead to performance degradations of the safety-related system. This includes conditions such as failures or consequential actions by systems that are NSR that could lead to spurious operation of both safety-related components and components that are NSR. For DI&C systems in plants that have IEEE Std 603-1991 as part of their licensing basis or for applications for CPs, OLs, SDAs, DCs, COLs, or MLs, the potential for spurious operation resulting from a CCF hazard of the DI&C system should be assessed using the following considerations:

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

b. For an A1 system, potential spurious operation of safety-related components or

components that are NSR due to CCF hazards can be adequately addressed through any combination of the following:

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

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

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

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

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

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

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

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

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

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

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

   iii For discrete B1 systems, the application should demonstrate that potential spurious operation of the control functions performed by each discrete B1

system is bounded by the accident analysis.

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

Acceptance Criteria

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

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

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

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

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

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

Displays and manual controls provided for compliance with Position 4 of the SRM on SECY-093-87, Item 18 should be sufficient both to monitor the plant state and to enable control room operators to actuate critical safety functions. For DI&C system modifications to operating plants, retention of existing analog displays and controls in the MCR could satisfy Position 4. However, if existing displays and controls are digital, or the same platform is used both for mitigating the DBE and to provide signals to these analog displays and controls, retaining existing analog displays and controls may not be sufficient to meet Position 4.

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

a. The 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.

The indication and manual controls to actuate these critical

~~h. If the D3 assessment reveals a potential for a CCF, then the method for accomplishing the diverse means of actuating the protective safety functions~~

should meet the following criteria: The diverse means should be:

a) at the system or division level (depending on the design);

b) initiated from the control room;

c) capable of responding with sufficient time available for the operators to determine the need for protective actions even with indicators that may be malfunctioning due to the CCF if credited in the D3 coping analysis;

d) appropriate for the event;

e) supported by sufficient instrumentation that indicates:

1. the protective function is needed,

2. the safety-related automated system did not perform the protective function, and

3. whether the automated diverse means or manual action is successful in performing the safety function.

(9) If the D3 assessment reveals a potential for a CCF, then, in accordance with the augmented quality guidance for the diverse means used to cope with a CCF, the design of a diverse automated or diverse manual actuation system should address how to minimize the potential for a spurious actuation of the protective system caused by the diverse means. Use of design techniques (for example, redundancy, conservative setpoint selection, coincidence logic, and use of quality components) to mitigate these concerns is recommended.

The adequacy of the diversity provided with respect to the above criteria should be justified by the applicant and explicitly addressed in the staff's safety evaluation.

~~3.2 RTS and ESFAS Interconnection~~

~~Interconnections between the RTS and ESFAS (for interlocks providing for reactor trip if certain ESFs are initiated, ESF initiation when a reactor trip occurs, or operating bypass functions) are permitted if it can be demonstrated that the functions required by the ATWS rule (10 CFR 50.62) are not impaired. Further, RTS and ESFAS could be combined into a single controller or central processing unit (CPU) provided D3 is adequately addressed to protect against CCF.~~

~~3.3 Single Failure and CCF~~

~~Since CCF is not classified as a single failure (as defined in RG 1.53), a postulated CCF need not be assumed to be a single failure in design basis evaluations. Consequently, realistic assumptions can be employed in performing analyses to evaluate the effect of CCF coincident with DBEs.~~

~~3.4 Use of Automation in Diverse Means~~

~~If automation is used in the diverse means, then the functions should be provided by equipment that is not affected by the postulated CCF and should be sufficient to maintain plant conditions within recommended acceptance criteria for the particular AOO or postulated accident. The automated diverse means may be performed by a nonsafety system, if the system is of sufficient quality to perform the necessary function(s) under the associated event conditions. The automated diverse means should be similar in quality to systems required by the ATWS rule (10 CFR 50.62), as described in the enclosure to GL 85-06, "Quality Assurance Guidance for ATWS Equipment that is Not Safety-Related." Other 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 the augmented quality discussed above.~~

~~3.5 Use of Manual Action as a Diverse Means of Accomplishing Safety Functions~~

~~If manual operator actions are used as the diverse means or as part of the diverse means to accomplish a safety function, a suitable HFE analysis should be performed by the applicant to demonstrate that plant conditions can be maintained within recommended acceptance criteria for the particular AOO or postulated accident. The acceptability of such actions is to be reviewed by the NRC staff in accordance with Appendix 18-A of SRP Chapter 18, "Crediting Manual Operator Actions in Diversity and Defense-in-Depth (D3) Analyses."~~

~~Note: As the difference between Time Available and Time Required for operator action is a measure of the safety margin and as it decreases, uncertainty in the estimate of the difference between these times should be appropriately considered. This uncertainty could reduce the level of assurance and potentially invalidate a conclusion that operators can perform the action reliably within the time available. For complex situations and for actions with limited margin,~~

~~such as less than 30 minutes between time available and time required, a more focused staff review will be performed.~~

b. ~~Diverse manual initiation of~~ 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 that the equipment is reliable and of sufficient quality. This equipment should be similar in quality to that required by the ATWS rule (i.e., 10 CFR 50.62), as described in the enclosure to Generic Letter 85-06.

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

Once ~~performed~~system- 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 the SRM on ~~a~~SECY-93-087, Item 18, if the application demonstrates the following acceptance criteria have been met:

a. The displays and controls are sufficient for the operator to monitor and control the critical safety functions.

b. The manual controls for these critical safety functions are at the system ~~level~~ or division level ~~basis (depending on~~and located within the ~~design).~~MCR. Since single failures concurrent with a CCF ~~are~~do not ~~required~~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 ~~should apply to at least one division that is in service (see section B.3.1, Item 9, concerning addressing spurious actuation caused by the diverse means in the design of the diverse means). A CCF that affects normal displays or controls should not prevent the operator from manually initiating safety functions. Prioritization between safety and diverse nonsafety systems to ensure the credited safety function can be accomplished by either system is addressed as follows:~~applies to at least one division that is in service.

~~Safety-related commands that direct a component to a safe state must always have the highest priority and must override all other commands. Commands that originate in a~~

~~safety-related channel but which only cancel or enable cancellation of the effect of the safe-state command (that is, a consequence of a CCF in the primary system that erroneously forces the plant equipment to a state that is different from the designated "safe state,") and which do not directly support any safety function, have lower priority and may be overridden by other commands. The reasoning behind the proposed priority ranking should be explained in detail. The reviewer should refer the proposed priority ranking and the explanation to appropriate systems experts for review. The priority module itself should be shown to apply the commands correctly in order of their priority rankings, and should meet all other applicable guidance. It should be shown that the unavailability or spurious operation of the actuated device is accounted for in, or bounded by, the plant safety analysis.~~

~~This recommendation does not prohibit the use of manual controls for operating individual safety system components after the corresponding safety system functions have been actuated.~~

~~3.6 Applicability to Current or New Plants~~

~~This guidance applies to both the currently operating NPPs licensed under 10 CFR Part 50 and new NPPs licensed under 10 CFR Part 52. The potential for CCF in digital safety systems should be considered whether the systems are to be used in new plants or for upgrades in existing plants. The main difference is that new NPPs predominantly will use digital technology, whereas currently operating plants may introduce digital upgrades in a phased approach. Therefore, Point 4 applies to new plants and to existing plants installing digital equipment in the RTS or ESF.~~

~~3.7 Effects of Spurious Actuation Caused by CCF~~

~~In cases in which a credible postulated spurious actuation(s) caused by a software CCF is not evaluated in design basis accident analyses, an analysis should be performed to determine whether such a postulated spurious actuation results in a plant response that falls outside the values or ranges of values chosen for controlling parameters as reference bounds for design. Further, the analysis should identify whether coping strategies exist for these postulated spurious actuations and consider the adequacy of such strategies. An applicant or licensee should confirm that a coping strategy has been identified to address the effects from credible spurious actuations caused by a CCF that have the potential to place the plant in a configuration that is not bounded by the plant design basis accident analyses.~~

~~3.8 Diversity Types~~

c. If equipment that is NSR 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 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

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

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, the results of the D3 assessment, specifically, the following:

1. Identification of any credited design attribute or defensive measure to eliminate CCF hazards from further consideration and a demonstration that these attributes or measures are effective. Identification of any remaining vulnerabilities to CCF hazards.

2. For CCF hazards that have not been eliminated from further consideration, 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 CCF hazard, the NRC staff should review the information provided to demonstrate the effectiveness of the diverse means, including any HFE analysis associated with manual operator action as a diverse means.

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

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

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

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

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

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

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

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

2. Vulnerabilities to potential spurious operations due to a CCF hazard in an A2 or B1 system have been addressed through use of a combination of the three factors described in Section B.4; or

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

f. For a proposed A1 system, design information showing that controls and displays:

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

2. Are diverse from the A1 system such that they are not subject to the same CCF hazard as the A1 system; and

3. Have adequate quality to support the manual operator action during the associated event condition if the equipment used is NSR.

~~NUREG/CR-6303 provides a method for determining uncompensated CCF in safety system designs. Section 2.6, "Diversity," of NUREG/CR-6303 defines six diversity attributes and 25 related diversity criteria. When NUREG/CR-6303 was published (December 1994,) computer-based digital systems were assumed to comprise the next generation of safety systems. Proposed safety system designs, however, include digital systems that are not computer-based, such as programmable logic devices, field programmable gate arrays, and application-specific integrated circuits. These digital devices and components use software to develop the logic that later resides within the digital component (called "firmware") and often cannot be changed in an individual component. These all should be considered in the assessment of diversity.~~

~~NUREG/CR-6303, Section 3.2, describes six types of diversity and describes how instances of different types of diversity might be combined into an overall case for the sufficiency of the~~

diversity provided. Typically, several types of diversity should exist, some of which should exhibit one or more of the stronger attributes listed in NUREG/CR-6303. Functional diversity and signal diversity are considered to be particularly effective. The following cautions should be noted where applicable:

- The justification for equipment diversity, or for the diversity of related system logic such as a real-time operating system, should extend to the equipment's components to assure that actual diversity exists. For example, different manufacturers might use the same processor or license the same operating system, thereby incorporating common failure causes. Claims for diversity on the basis of the difference in manufacturer name are insufficient without consideration of the above.

  With respect to computer software and software-based logic diversity, experience indicates that independence of failure causes may not be achieved in cases where multiple versions of software, for example, are developed using the same set of software, system, and logic development tools. Other considerations, such as technology, functional and signal diversity that lead to different software, system, and logic requirements form a stronger basis for diversity.

3.9 System Testability

If a portion or component of a system can be fully tested, then it can be considered not to have a potential for software-based CCF. Fully tested or 100 percent testing means that every possible combination of inputs and every possible sequence of device states are tested, and all outputs are verified for every case. Further, in assessing the system states, the guidance provided in IEEE Std 7-4.3.2, Clause 5.4.1, "Computer System [Equipment Qualification] Testing," should be addressed:

> Computer system [equipment] qualification testing (see 3.1.36) shall be performed with the computer functioning with software and diagnostics that are representative of those used in actual operation. All portions of the computer necessary to accomplish safety functions, or those portions whose operation or failure could impair safety functions, shall be exercised during testing. This includes, as appropriate, exercising and monitoring the memory, the CPU, inputs and outputs, display functions, diagnostics, associated components, communication paths, and interfaces. Testing shall demonstrate that the performance requirements related to safety functions have been met.

The use of the term "software" or "software-based" should be extended to any form of logic that is used in a safety system to accomplish a safety system function and relies upon the use of software for its development. Similarly, the use of the phrase "All portions of a computer" should be extended to "All components of a safety system relying upon a software development system."

~~Clause 5.4.1 of IEEE Std 7-4.3.2 directs the system developer or user to perform equipment qualification of the system (i.e., hardware and software) in its operational states while the system is operating at the limits of its equipment qualification envelope. The logic and diagnostics should be representative of the logic used in actual operation to a degree that provides assurance that the system states produced by the actual system will be tested during the equipment qualification process.~~

~~3.10 Displays and Manual Controls~~

~~Displays and manual controls provided for compliance with Point 4 of the NRC position on D3 should be sufficient both for monitoring the plant state and to enable control room operators to actuate systems that will place the plant in a safe shutdown condition. In addition, the displays and controls should be sufficient for the operator to monitor and control the following critical safety functions: reactivity level, core heat removal, reactor coolant inventory, containment isolation, and containment integrity. These displays and controls provide plant operators with information and control capabilities that are not subject to CCF due to errors in the plant automatic DI&C safety systems because the displays and controls are independent and diverse from the safety system.~~

~~The point at which the manual controls are connected to safety equipment should be downstream of equipment that can be adversely affected by a CCF. These connections should not compromise the integrity of interconnecting cables and interfaces between local electrical or electronic cabinets and the plant's electromechanical equipment. To achieve system-level actuation at the lowest possible level in the safety system architecture, the controls may be connected either to discrete hardwired components or to simple (e.g., component function can be completely demonstrated by test,) dedicated, and diverse, software-based digital equipment that performs the coordinated actuation logic.~~

~~The displays may include digital components that are not adversely affected by a CCF of the safety functions credited in the accident analysis. Functional characteristics (e.g., range, accuracy, time response) should be sufficient to provide operators with the information needed to place and maintain a plant in a safe shutdown condition.~~

~~HFE principles and criteria should be applied to the selection and design of the displays and controls. Human performance requirements should be described and related to the plant safety criteria. Recognized human factors standards and design techniques should be employed to support the described human performance requirements.~~

8. ~~4.~~ Review Procedures

In reviewing the ~~applicant's~~ D3 ~~analysis using~~assessment results in accordance with the ~~above~~ acceptance criteria described in Section B.3 of this BTP and the detailed guidance of NUREG/CR~~-~~6303 and NUREG/CR-7007, emphasis should be given to the ~~following~~ topics described below:

8.1. ~~4.1~~ System Representation as Blocks

The system being assessed is represented as a block diagram; the inner workings of the blocks are not necessarily shown. ~~Diversity is determined at the block level.~~ 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/subroutine, such as voting block or proportional-integral-derivative block, that is used by multiple functional applications; a design or implementation defect in this type of block can result in a CCF hazard of all application functions that utilize that block. Diversity is determined at the block level.

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

8.2. ~~4.2~~ Documentation of Assumptions

~~Assumptions~~ The application documents any assumptions made to compensate for missing information in the design description materials or to explain ~~particular~~ interpretations of the analysis guidelines as applied to the system ~~are documented by the applicant~~.

~~4.3 Exclusion of Components from D3 Analysis~~

~~A software-based component may be sufficiently simple and deterministic in performance such that the component is not a source of a CCF. Such components need not be considered in a D3 analysis. When a basis is given that a component is not susceptible to CCF, the NRC staff should examine the justification carefully.~~

8.3. ~~4.4~~ Effect of Other Blocks

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

8.4. ~~4.5~~ Identification of Alternate Trip or Initiation Sequences

~~Thermal~~ 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 ESF ~~are included in the assessment. (~~. Coordination with the organization responsible for the review of reactor systems is necessary in reviewing these analyses~~.)~~.

8.5. ~~4.6~~ 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 CCF hazard 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 operator action is cited as the diverse means for response to an event, the applicant should demonstrate that the HFE analysis is adequate ~~information (indication), appropriate operator training, and sufficient time for operator action are available~~ in accordance with ~~Appendix 18-A of~~ SRP Chapter ~~18~~ 18. Coordination with the organization responsible for the review of human-system interfaces for any credited diverse manual operator action should be included as part of this activity.

~~Note: As the difference between Time Available and Time Required for operator action is a measure of the safety margin and as it decreases, uncertainty in the estimate of the difference between these times should be appropriately considered. This uncertainty could reduce the level of assurance and potentially invalidate a conclusion that operators can perform the action reliably within the time available. For complex situations and for actions with limited margin, such as less than 30 minutes between time available and time required, a more focused staff review will be performed.~~

8.6. ~~4.7~~ Justification for Not Correcting Specific Vulnerabilities

~~If~~Justification should be provided for not correcting any identified vulnerabilities ~~are~~ not addressed by other aspects of the application such as design ~~modification, refined analyses~~attributes, defensive measures, or provision of alternate trip, initiation, or mitigation capability~~, justification should be provided~~. This includes any NRC-approved credited operator action taken to prevent the AOO or postulated accident from occurring. These justifications will be reviewed on a case-by-case basis.

C. REFERENCES

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

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

~~2.~~3. Institute of Electrical & Electronics Engineers, IEEE Std 279-1971, “Criteria for Protection Systems for Nuclear Power Generating Stations,” Piscataway, NJ.

~~3.~~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.

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

5.6. Institute of Electrical & Electronics Engineers, IEEE Std. 7-4.3.2, "IEEE 603-1991, "Standard Criteria for Digital Computers in Safety Systems infor Nuclear Power Generating Stations," Piscataway, NJCorrection Sheet, January 30, 1995.

6.1. U.S. Nuclear Regulatory Commission, "Task Working Group No. 2: Diversity andA Defense in-Depth Issues Interim Staff Guidance," DI&C-ISG-02, Revision 2, June 5, 2009-in-.

7. U.S. Nuclear Regulatory Commission, "Quality Assurance Guidance for ATWS Equipment that is not Safety-Related," Generic Letter 85-06, April 16, 1985.

8. U.S. Nuclear Regulatory Commission, "Crediting Manual Operator Actions in Diversity and Defense-in-Depth (D3) Analyses," NUREG-0800, SRP Chapter 18, Appendix 18-A.

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

10. U.S. Nuclear Regulatory Commission, "Clarification of TMI Action Plan Requirements (GL No. 82-33)," December 17, 1982.

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

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

13.8. U.S. Nuclear Regulatory Commission, "Application of the Single-Failure Criterion to Nuclear Power Plant ProtectionSafety Systems,"," Regulatory Guide 1.53.

14.9. U.S. Nuclear Regulatory Commission, "Criteria for Use of Computers in SafetyControl Systems of Nuclear Power Plants," Regulatory Guide 1.152," NUREG-0800, SRP Section 7.7.

15. U.S. Nuclear Regulatory Commission, "Manual Initiation of Protective Actions," Regulatory Guide 1.62.

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

11. U.S. Nuclear Regulatory Commission, "Diverse Instrumentation and Control Systems,"

NUREG-0800, SRP Section 7.8.

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

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

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

~~17.~~15. 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.~~16. U.S. Nuclear Regulatory Commission, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-~~-~~Water Reactor (ALWR) Designs," SRM ~~on~~for SECY-~~-~~93-~~-~~087, July ~~-~~ 21, 1993.

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

U.S. Nuclear Regulatory Commission, "Quality Assurance Guidance for ATWS Equipment

~~**PAPERWORK REDUCTION ACT STATEMENT**~~

~~The information collections contained in the Standard Review Plan are covered by the requirements of 10 CFR 50, 10 CFR 52 and 10 CFR 100, and were approved by the Office of Management and Budget, approval number 3150-0011, 3150-0151, and 3150-0093.~~

~~**PUBLIC PROTECTION NOTIFICATION**~~

18. That Is Not Safety-Related," Generic Letter 85-06, April 16, 1985.

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

Paperwork Reduction Act Statement

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

Public Protection Notification

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

BTP Section 7-19

Description of Changes

~~**BTP 7-19, "Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems"**~~

BTP 7-19, "GUIDANCE FOR EVALUATION OF COMMON CAUSE FAILURE HAZARDS DUE LATENT SOFTWARE DEFECTS IN DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS"

This BTP section updates the guidance previously provided in Revision ~~6~~7, dated ~~July 2012. See~~ August 2016 (Agencywide Documents and Management System (ADAMS) Accession No. ~~ML110550791.~~ ML16019A344).

~~The main purpose of this update is to incorporate the revised software RGs and the associated endorsed standards. For organizational purposes, the revision number of each RG and year of each endorsed standard is now listed in one place, Table 7-1. As a result, revisions of RGs and years of endorsed standards were removed from this section, if applicable. For standards that are incorporated by reference into regulation (IEEE Std 279-1971 and IEEE Std 603-1991) and standards that have not been endorsed by the agency, the associated revision number or year is still listed in the discussion. Additional changes were editorial.~~

~~Part of 10 CFR was reorganized due to a rulemaking in the fall of 2014. Quality requirement discussions in the former 10 CFR 50.55a(a)(1) were moved to 10 CFR 50.54(jj) and 10 CFR 50.55(i). The incorporation by reference language in the former 10 CFR 50.55a(h)(1) was moved to 10 CFR 50.55a(a)(2). There were no changes either to 10 CFR 50.55a(h)(2) or 10 CFR 50.55a(h)(3).~~

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 hazards caused by CCFs of digital technology, in particular within software or software-based logic. This update clarifies the scope of applicability for all users as well as clearly stating the applicability of this guidance to the 10 CFR 50.59 change process. The update provides for a graded approach that clarifies the technical rigor and analysis that's appropriate for SSCs of differing safety class so that an adequate demonstration of safety for a proposed modification is consistently applied. This is in addition to clarifying specific areas of guidance such as diversity and testing to eliminate further consideration of CCF hazards. Lastly, the update revises the flow and structure of the BTP's guidance to improve readability so that the user clearly understands the overall process for addressing CCF hazards.