From:	Govan, Tekia
To:	Govan, Tekia
Subject:	Commented Line-by-line Mark-up of BTP 7-19 from an Anonymous Commenter
Date:	Thursday, August 29, 2019 12:31:08 PM
Attachments:	Summary of Key Comments on the Staffs Proposed BTP 7-19 Rev 8.pdf Line-by-Line Comments on Staff"s Proposed Draft BTP 7-19 Revision 8_for 8-29-2019 Public Meeting _Anonymous1.pdf

---

From: Rahn, David
Sent: Thursday, August 29, 2019 8:47 AM
To: Govan, Tekia <Tekia.Govan@nrc.gov>
Cc: Morton, Wendell <Wendell.Morton@nrc.gov>; Alvarado, Rossnyev <Rossnyev.Alvarado@nrc.gov>; Zhang, Deanna <Deanna.Zhang@nrc.gov>; Rebstock, Paul <Paul.Rebstock@nrc.gov>
Subject: FW: Commented Line-by-line Mark-up of BTP 7-19 from an Anonymous Commenter

Hi Tekia:

Late last night I received a package with two attachments:

a. A Line-by-line mark-up of the staff's proposed Draft Rev. 8 to BTP 7-19, and
b. A summary of the key comments within the mark-up.

The sender wishes to remain anonymous.

I will mention that we received comments on the Draft BTP revision from parties that are not affiliated with NEI, and that these comments will be included within the meeting summary.

Dave

Comments on the NRC Staff's Proposed Draft 8 to SRP Section BTP 7-19

This is a summary of our key comments:

1. The distinction between a D3 assessment and Qualitative assessment is unclear and unnecessary. For A1, A2 and B1 systems a CCF vulnerability assessment is required, and a plant safety assessment is needed for any CCFs that are not prevented. The only difference is that the defensive measures that can be credited to reach a "no CCF" conclusion for a design defect in A1 systems are prescriptive – sufficient internal diversity or sufficient testability; the defensive measures that can be credited for A2 and B1 systems are not prescriptive and can be identified and defended by the licensee. I've said this in one sentence, the current draft requires more than 30 pages to say this.

2. The document defines "best estimate" as allowing relaxed initial conditions, but for previous digital systems "best estimate" has also meant relaxed acceptance criteria, and qualitative assessments by safety analysis experts vs. quantitative assessments using computer codes.

3. Nowhere in this document does it say that an AOO or PA with concurrent LOOP and concurrent digital CCF does not need to be considered. This has been accepted by the staff for all previous digital safety system reviews; it is essential to a manageable CCF strategy. There is no practical technical solution to managing this multiple CCF scenario (LOOP is a CCF).

4. The document casually mentions single failures that can lead to CCFs in integrated digital systems. But these CCFs should be emphasized, because they are much more troublesome than CCFs due to a design defect. Single failures are expected during the life of the plant; therefore, they are within the plant's design basis. If there are inadequate defensive measures to prevent these CCFs, conservative quantitative plant safety analysis is required. Most important is that these CCFs can cause unbounded plant transients that must be identified in the FSAR as new AOOs.

U.S. NUCLEAR REGULATORY COMMISSION

STANDARD REVIEW PLAN

BRANCH TECHNICAL POSITION 7-19

GUIDANCE FOR EVALUATION OF POTENTIAL COMMON CAUSE FAILURE IN DIGITAL 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) and the years of endorsed industry standards referenced in this branch technical position (BTP) are centrally maintained in Standard Review Plan (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 regulation (Institute of Electrical and Electronics Engineers (IEEE) Standard (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

Common cause failures (CCF) have been identified as a type of hazard that digital I&C (DI&C) systems could be more susceptible to due to the integration capabilities provided by the technology and its inherent complexity compared to analog technologies [If you don't add complexity you leave an argument that if there is no integration there is no potential for CCF. But even non-integrated components can have a design defect.]. DI&C systems can also be vulnerable to a CCF caused by design errors, including digital hardware design errors, software errors or errors in software developed logic. A CCF in a DI&C system can result in loss of a safety function either through 1) systematic faults within redundant portions (e.g., safety divisions) of a safety-related system; 2) propagation of faults between safety divisions or from systems that are not safety-related to safety-related systems; or 3) internal or external plant hazards (e.g., electro-magnetic interference). The latter two sources of CCF are primarily

addressed through providing independence between safety divisions and between safety-related and systems that are not safety-related, and qualification of DI&C equipment, respectively. Independence encompasses physical independence, electrical independence, communications independence and functional independence. Systematic faults are latent defects in hardware, software, or system components that can be triggered by an event or condition. A CCF of a DI&C system can result in loss of a safety function during a design-basis event (DBE). A ~~CCF of a~~ DI&C system fault can also actuate a safety-related function or other design function~~s~~ without a valid demand. A DI&C system fault can also result in erroneous system actions. ~~This~~ These condition~~s~~ ~~is~~ are typically referred to as spurious operation but can be used interchangeably with the term spurious actuation. When a DI&C fault adversely affects multiple SSCs it is referred to as a CCF.

In NUREG-0493, "A Defense-in-Depth and Diversity Assessment of the RESAR-414 Integrated Protection System," the U.S. Nuclear Regulatory Commission (NRC) staff documented a defense-in-depth and diversity (D3) assessment of a digital computer-based reactor protection system (RPS) in which defense against software CCF (or simply CCF hereafter) that 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 RPS consisted of the reactor trip system and the engineered safety features (ESF) actuation system. Subsequently, in SECY-91-292, "Digital Computer Systems for Advanced Light-Water Reactors," the NRC staff included discussion of its concerns about CCF in digital systems used in nuclear power plants (NPP).

As a result of reviews of applications for certification of evolutionary and advanced light-water reactor (LWR) designs using DI&C systems, the NRC staff documented its position ~~with respect to~~regarding vulnerabilities to CCF ~~due to latent software defects~~ [there is no mention of software] in DI&C systems and D3 to address those vulnerabilities in Item II.Q, in SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs." The Commission subsequently modified this position in the associated staff requirements memorandum (SRM), Item 18, in which it indicated that a CCF ~~due to latent software defects~~ of a DI&C safety system is considered ~~the~~ a beyond design basis event (BDBE). This conclusion was based primarily on the robust design processes required for safety systems, which reduces the likelihood of a hidden design defect to a level that is much lower than a design basis events (DBE), but no so low as to require no further consideration (as was the case for a design defect in prior analog systems).

The NRC staff provided plans to clarify the guidance associated with addressing potential CCF of DI&C systems in SECY-18-0090, "Plan for Addressing Potential Common Cause Failure in Digital Instrumentation and Controls." This SECY paper documented the NRC staff's evaluation of the SRM on SECY-93-087. The staff concluded that the SRM on SECY-93-087 provides adequate flexibility for regulatory modernization activities that support near-term DI&C implementation. SECY-18-0090 outlines five guiding principles to ensure consistent application of the direction provided in SRM-SECY-93-087. These guiding principles provide a framework for addressing potential CCF in DI&C systems using a graded approach based on safety significance of the DI&C system. In this SECY paper, the NRC staff committed to incorporating these guiding principles into the NRC staff's review guidance. In summary, while the NRC considers CCF ~~due to software~~ that leads to loss of the safety function in multiple independent ~~in~~ DI&C safety ~~systems~~ divisions to be beyond the design-basis, applicants and licensees

should evaluate the potential for this CCF ~~due to software~~ in DI&C systems and verify that the plant is protected from the effects of these potential CCFs. In addition, applicants and licensees should evaluate sources of CCF that can result in spurious operations, some of which may be DBEs, as discussed later in this BTP. Over the years, NRC staff has approved numerous design solutions (sometimes multiple design solutions for a single DI&C system) employed by licensees and applicants to address potential CCF in DI&C systems. This BTP provides guidance for reviewing the applicant or licensee's design and analysis for addressing potential CCFs ~~due to latent software defects~~ in ~~the~~ I&C systems.

1. Regulatory Basis

- For applications filed after May 13, 1999, Title 10 of the *Code of Federal Regulations* (10 CFR) 50.55a(h), "Protection and Safety Systems," 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 279-1968, "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." This BTP is applicable to digital upgrades in all plants [maybe not here, but someplace in this document].

- 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 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 279-1968, Clause 4.2, requires in part that "any single failure within the protection system shall not prevent proper protection system action when required."

- 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 no single failure results in the loss of the protection function."

- GDC 21, "Protection System Reliability and Testability" states in part, "the protection system shall be designed for high functional reliability and inservice testability commensurate with the safety functions to be performed."

- GDC 22, "Protection System Independence," requires in part "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 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 26, "Reactivity Control System Redundancy and Capability," requires, in part, two independent reactivity control systems of different design principles to be provided.

- 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 applications for early site permits, standard design certifcation, 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 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.

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

  - 10 CFR 50.34(a)(1)(ii)(D) provides guideline values for CP applicants and NPPs licensed to operate under Part 50 after January 10, 1997.

  - 10 CFR 52.47(a)(2)(iv) provides guideline values for standard DCs.

  - 10 CFR 52.79(a)(1)(vi) provides guideline values for COLs.

  - 10 CFR 52.137(a)(2)(iv) provides guideline values for SDAs.

  - 10 CFR 52.157(d) provides guideline values for ML approvals.

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, "Application of the Single-Failure Criterion to Nuclear Power Generating

Station Safety Systems," Clause 5.5, establishes the relationship between CCF and single failures by defining criteria for CCFs that are not subject to single-failure analysis; depending on the source of these CCFs they are considered beyond design basis events (BDBE) or are excluded from further consideration, as discussed in this BTP .

- NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems," 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 that could occur within digital (computer-based) RPSs and determines what portions of a design need to implement additional diversity or defense-in-depth measures to address such failures.

- SECY-93-087, Item II.Q, as clarified by the SRM on SECY-93-087, Item 18, II.Q, describes the NRC position.

- Generic Letter (GL) 85-06, "Quality Assurance Guidance for ATWS Equipment that is not Safety-Related," April 16, 1985, provides quality assurance guidance for anticipated transient without scram (ATWS) equipment that is not safety-related.

- SECY-18-0090, "Plan for Addressing Common Cause Failure in Digital Instrumentation and Controls" provides the NRC staff's plan to clarify the guidance associated with evaluating and addressing potential CCF of DI&C systems.

- Regulatory Information Summary (RIS) 2002-22, Supplement 1, "Clarification on Endorsement of Nuclear Energy Institute Guidance in Designing Digital Upgrades in Instrumentation and Control Systems" clarifies guidance for preparing and documenting "qualitative assessments" that can be used to evaluate the likelihood of failure of a proposed digital modification.

- NUREG-0800, SRP Chapter 18, Appendix 18-A, "Crediting Manual Operator Actions in Diversity and Defense-in-Depth Analyses," defines a methodology, applicable to both existing and new reactors, for evaluating manual operator actions as a diverse means of coping with anticipated operational occurrences (AOO) and postulated accidents that are concurrent with a software CCF of the DI&C protection system.

- 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.

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, operating licenses, COLs, and design certifications, SDAs and MLs. While t~~T~~his BTP is not applicable for ~~proposed~~

modifications performed under the 10 CFR 50.59 change process, the technical positions are applicable to all digital systems.

4. Purpose

The purpose of this BTP is to provide guidance for reviewing a licensee or applicant's evaluation of 1) a DI&C system's vulnerability to CCF due to latent defects in the hardware, software or software-based logic, including the measures implemented to prevent or limit the effects of the CCF; 2) the effects of such a CCF on plant safety, including the methods credited to cope with a CCF that is not prevented; and 3) the measures implemented to limit, mitigate, or cope with the effects of the CCF [changed to reflect a two part evaluation, as discussed later.]. This BTP provides guidance on implementing a graded approach to address the potential for CCF due to latent design 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[1] and logic developed from software-based development systems (e.g., Hardware Description Language Programmed Devices).

This BTP is primarily intended to address CCFs caused by a digital design defect, which is considered a beyond-design-basis event (BDBE) for SSCs that employ a robust design process to reduce the likelihood of design defects. The plant-level results of BDBEs may be analyzed using best-estimate methods. However, in integrated digital systems, a single random hardware failure can result in a CCF that have cascading adversely eaffects multiple SSCs, similar to a CCF (e.g. loss of multiple functions within a safety or non-safety groupsystem [group is not defined], or spurious operation of functions within multiple safety or non-safety groupssystems). Single random hardware failures with cascading effectsthat result in CCFs are considered design basis events (DBEs), because random hardware failures are expected during the life of the plant. DBEswhose plant-level results call for conservative deterministic analysis methods to demonstrate that they plant level results are bounded by existing identified AOOs, or have acceptable results for any new or unbounded AOOs that are identified through the analysis. RG 1.53 provides guidance for the deterministic analysis of single failures in safety-related systems. A graded approach to this analysis may be applied to systems that are not safety-related [non-safety systems added above.].

This BTP provides guidance for reviewing design measures such as the use of diverse equipment within a system to prevent a CCF, diverse external equipment, including manual controls and displays, to mitigate a CCF, and other design attributes to ensure conformance with the NRC's position on addressing potential CCFs in digital I&C systems as specified in the SRM on SECY-93-087 with clarifications provided in SECY-18-0090. The objective of this review is to:

- Verify that vulnerabilities to CCF have been adequately identified and addressed for DI&C systems.

- Verify that an adequate D3 assessment, consisting of an evaluation of the credibility of a

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

CCF occurrence, followed by an assessment of the consequences of credible CCFs, has been performed for proposed DI&C systems of high safety significance to meet the criteria established by NRC guidance.

- Verify that a qualitative assessment of likelihood [You are distinguishing "credibility" in the bullet above and "likelihood" in this bullet, but you are not defining the difference. This is just going to continue to cause industry confusion.] of occurrence of CCFs has been performed for proposed DI&C systems of lower safety significance, based on defensive design measures and quality development processes that have been incorporated into such lower safety-significant DI&C systems. Followed by an assessment of the consequences of CCFs that are not prevented.

[In the two bullets above you are trying to distinguish the process for systems of high and lower safety significance. But the process is the same. In both cases you must assess the likelihood of the CCF, then assess the consequences for any CCFs that are not prevented. The only difference is in the conservatism of the defensive measures that can be credited for CCF prevention or likelihood reduction. For high safety significant systems, the defensive measures must be more deterministic; for lower safety significant systems defensive measures can be more qualitative. If you explain it this way, removing the distinction between a "D3 assessment" label and the "qualitative assessment" label, it would be much easier for industry to understand.]

- Verify that if defensive measures are used in a proposed DI&C system to prevent a CCF, reduce the likelihood of CCF or limit its consequences, the measures are adequate depending on the systems safety significance.

- Verify that if diversity has been provided in a design to ~~meet the criteria established by NRC guidance~~prevent a CCF, ensure non-concurrent triggers or mitigate a CCF, the diversity measures are adequate depending on the systems safety significance.

- Verify that if ~~a diverse~~ manual means ~~of performing the function(s) is used~~are credited to ~~address the potential occurrence of~~mitigate a CCF ~~of the automatic DI&C systems~~, the ~~independent~~ prompting alarms, displays and manual controls to be used by the operator ~~to achieve the credited safety functions~~ are not subject to the same CCF source and the time margin for crediting manual controls meets the criteria for manual controls established by NRC HFE guidance.

This BTP also addresses CCFs due to latent ~~software~~ digital defects that can cause spurious operation of a safety or non-safety function, because spurious operations have the potential ~~that could~~ to put the plant in an unanalyzed condition. If unanalyzed, ~~or a~~the condition ~~that cannot~~ may not be adequately mitigated by ~~a safety-related~~ [deleted because these are typically BDBEs] other I&C systems. This BTP provides criteria for analyzing such conditions, including using best-estimate methods and crediting non-safety systems.

B. BRANCH TECHNICAL POSITION

1. Introduction

1.1. Four CCF Positions and Clarification

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 positions stated in SRM-SECY-93-087 are quoted below:

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

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

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

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

SECY-18-0090 clarifies the application of the Commission's direction in the above four positions to reduce regulatory uncertainty. Position 1 of SRM on SECY-93-087, Item 18, II.Q specifies the required performance of a D3 assessment (see Section 3 below for a description of this assessment) to demonstrate that vulnerabilities to CCFs have been adequately addressed. The guiding principles within SECY-18-0090 clarify that the applicant or licensee could use a graded approach to determine the degree of rigor that is necessary to accomplish the D3 assessment. This graded approach is described in Section B.2.1 below. [You should stop trying to explain each point individually, but rather explain them in aggregate to align with the two steps described in the first paragraph of the "Purpose" section (1) assess vulnerability to CCF (2) assess plant safety for any CCF that is not prevented and results in a safety system failure concurrent with each AOO and PA. It is important to note that CCFs that result in spurious operations do not require consideration concurrent with each AOO or PA, because spurious operations are self-announcing; therefore, they can be corrected prior to a plant accident.]

The term "best-estimate methods" in Position 2 is now referred to as methods using "realistic

assumptions," which are defined as the initial plant conditions corresponding to the onset of the event being analyzed. For example, initial plant event conditions, such as:

- power levels,
- temperatures,
- pressures,
- flows, and
- alignment of equipment.

[As written, computer codes must still be used and the acceptance criteria is unchanged; only the initial conditions are different. This was not the interpretation for System 80+, US-APWR, APR1400 or Oconee RPS. For each of these "best estimate" also allowed qualitative safety analyst expert judgment to conclude that the event was bounded or did not cause breaches of fuel, containment or pressure boundaries that would exceed offsite radiation dose limits. Computer codes were rerun with new initial conditions, only when experts could not reach or defend a qualitative conclusion.]

The guiding principles within SECY-18-0090 clarify that in addition to "best-estimate methods" identified in Position 2 of SRM on SECY-93-087, Item 18, II.Q, the plant safety~~D3~~ assessment can be performed using a design-basis analysis (conservative methods). Thus, when performing the plant safety~~D3~~ assessment, the vendor or applicant should analyze each postulated CCF for each event that is evaluated in the SAR section analyzing ~~power operation~~ [There is no such limitation in the SECY. Limiting this to power operation events, is not consistent with the PRA which shows that lower power events are higher risk.] accidents at the design basis plant conditions corresponding to the onset of the event. This assessment may use realistic assumptions to analyze the plant response to DBEs, or the conservative assumptions on which the SAR analysis is based (normally documented in Chapter 15, but could be in other sections of the SAR). [Clarify that CCF must be assessed concurrent with loss of offsite power (LOOP) because LOOP is an AOO, but CCF with LOOP and another AOO/PA does not require assessment due to the aggregate extremely low likelihood (i.e., similar to an earthquake that exceeds the required DBE level.]

If the ~~D3~~ plant safety assessment indicates a postulated CCF could disable a safety function, then Position 3 directs that an applicant should identify an existing diverse means or add a diverse means to perform the safety function or a different function that provides adequate AOO/PA mitigation. The diverse means may be equipment that is not safety-related (see Section 3, "D3 Assessment") with a documented basis that the diverse means is of sufficient quality and unlikely to be subject to the same CCF. SECY-18-0090 clarifies that use of either an 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~~ plant safety assessment demonstrates that a CCF, when analyzed in the accident analysis section of the SAR, can be reasonably mitigated ~~through other means (such as~~ with current systems~~)~~, an added 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 that disabled the safety function.

If a diverse means is part of a safety division, 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. However, within a division independence is not required between the diverse means. If the diverse means is not safety-related, then the IEEE Std 603-1991, Clause 5.6.3 requirements for separation and independence between safety-related systems and non-safety related systems would apply.

Position 4 directs the inclusion of a set of displays and manual controls (safety or nonsafety[2]) in the MCR that is diverse from any CCF vulnerability identified within the "safety computer system" discussed in Positions 1 and 3 above and meets divisional independence requirements as applicable for the specific design implementation. These displays and controls are for manual, system or divisional level (depending on the design) actuation and control of equipment to manage the "critical safety functions" (see Section 1.2 below) even if they are not credited for CCF mitigation in the plant safety assessment. Further, ~~if not~~since they cannot be subject to the same CCF as the proposed safety-related digital ~~protection~~ [SECY 93-087 requires consideration of CCF in any system that is credited for AOO or PA mitigation. This goes well beyond the protection system, which is limited to RPS and ESFAS. Any system directly credited for AOO or PA mitigation is an A1 system. The limitation on the applicability of this BTP to only protection systems needs to be changed throughout this document.] system, ~~some of~~ these displays and manual controls from Position 4 may be credited as all or part of the diverse means called for under Position 3.

The Position 4 phrase ". . . safety computer system identified in Items 1 and 3 above" refers to the ~~automatic~~ safety-related DI&C system that is credited for DBE AOO/PA mitigation. This is typically automatic safety related functions, but for some events manual controls are credited. If the credited manual controls are digital and a CCF is not prevented, then a diverse means of event mitigation (automatic or manual) must be provided for the plant safety assessment. Diverse Position 4 controls must also be provided if the manual controls for which a CCF is not prevented are credited to manage the plant's critical safety functions.

The above four positions from the SRM on SECY-93-087, Item 18 II.Q is based on the NRC concern that ~~software-based or software-logic-based~~ DI&C systems development errors are a credible source of CCF. Generally, DI&C systems cannot be proven to be error-free ~~from a design and software development perspective~~due to the inherent complexity of digital technology. Therefore, DI&C systems are considered vulnerable to CCF because either 1) identical digital hardware designs and identical copies of the software or software-based logic are present in redundant divisions of safety-related systems; or 2) there exists integration of previously separate functions into a single DI&C system. ~~Also, some errors, such as those labeled as "software errors," actually result from errors in the higher-level requirements[3] specifications, in which the system design misrepresent the actual process.~~[If you introduce this, then there is no distinction between digital and analog systems. Analog systems could also have errors in higher level requirements.]

[2] While the SRM on SECY-93-087 uses the term "nonsafety," the NRC staff interprets this as not safety-related.

[3] As used here, the term "higher-level requirements" and the like do not refer to NRC regulatory requirements, but to system or component design or operating characteristics upon which the licensee relies to accomplish the stated system or component safety functions. Throughout this BTP, context will indicate whether requirements are NRC regulatory requirements or "higher-level requirements" as explained in this footnote.

SECY-18-0090 recognizes that although significant effort has been applied to the development of highly reliable DI&C systems, the NRC staff believes that some residual faults might remain undetected within a system and could result in hazards that can challenge plant safety. This includes hazards that result from loss of the safety function or those caused by spurious operation of a safety or non-safety function. To address these potential hazards, the NRC staff should verify that applicants and licensees have 1) identified potential hazards due to ~~CCF~~ a design defect in ~~the software or software-based logic of~~ a DI&C system and associated impacts to the intended design functions and prevented a CCF ; and 2) for CCFs that are not prevented, assess~~ed~~ the ability of the overall plant design (e.g., I&C systems, mechanical systems and manual operator actions) to ~~perform its intended design functions or demonstrate the plant safety analysis assumptions remain valid~~ maintain plant safety, using conservative or "best-estimate" methods.

1.2. Critical Safety Functions

SECY-93-087, Item II.Q, [critical functions are defined in NUREG 0737, not SECY 93-087] defines critical safety functions as the following:

- Reactivity control
- Core heat removal
- Reactor coolant inventory
- Containment isolation
- ~~Containment Isolation~~Radioactivity control

Therefore, a safety function identified in the plant safety analysis may not always be a critical safety function.
[I think this section is attempting to define the critical safety functions for Position 4. But there is currently no correlation to Position 4.

2. Graded Approach and Level of Integration for Addressing CCF

2.1. Graded Approach for Categorizing Digital I&C Systems

For assessing vulnerabilities to CCF, a graded approach refers to analyses performed for equipment of differing safety significance in which CCF concerns apply. For example, a CCF analysis for a digital reactor trip system would be expected to be more rigorous than a CCF analysis for a safety-related MCR HVAC chiller. [I disagree. The analysis should be the same. Both require a CCF vulnerability assessment and a plant safety assessment for CCFs that are not prevented. The only difference should be in the conservatism required to credit defensive measures that prevent a CCF. you can greatly simplify this BTP.] Table 2-1 depicts a categorization scheme for implementation of this graded approach that is based on the classification of the DI&C system and its safety significance.

Table 2-1: Categorization Scheme for Implementing A Graded Approach to Address CCF

	Safety-Related	Not Safety-Related
Safety Significant – Significant Contributor to Plant Safety	**A1**	**B1**
Not Safety Significant – Not a significant contributor to plant safety	**A2**	**B2**

The following criteria should be used to determine the category of a DI&C system:

a. A1: Safety-related DI&C system: [this should be simplified to safety related systems/components directly credited for AOO or PA mitigation or to achieve safe shutdown]

   1. that is relied upon to initiate and complete control actions essential to maintain plant parameters within acceptable limits established for a DBE; or
   2. whose failure could directly lead to accident conditions that may cause unacceptable consequences (i.e., exceeds acceptable limits for a DBE) if not mitigated by other A1 systems.

b. A2: Safety-related DI&C system that: [this should be simplified to all other safety related systems/components]

   1. provides an auxiliary or indirect function in the achievement or maintenance of plant safety; or
   2. maintains the plant in a safe shutdown state after the plant has reached initial safe shutdown state.

c. B1: DI&C system that is not safety-related: [should be simplified to non-safety related systems/components whose failure (including spurious operation) would result in an AOO or challenge to a critical safety function, assuming no other mitigating actions]

   1. that directly affects the reactivity or power level of the reactor, or affects the integrity of the safety barriers (fuel cladding, reactor vessel, or containment); or
   2. whose failure may result in unacceptable consequences to plant safety due to integration of multiple control functions into a single system.

d. B2: DI&C system that is not safety-related: [should be simplified to all other non-safety systems/components]

1. that does not have a direct effect on reactivity or power level of the reactor; and
2. whose failure does not have consequences to plant safety or whose failure can be detected and mitigated with significant safety margin.

The application should document the basis for categorizing each DI&C system.

The application should address following criteria regarding the potential for CCFs in the proposed system:

a. For an A1 system, the application should include a ~~D3~~ CCF assessment and plant safety assessment in accordance with the criteria in Section B.3.1.

b. For an A2 or B1 system, the application should include a CCF assessment and plant safety ~~qualitative~~ assessment in accordance with Section B.4 to address potential CCFs.

c. For a B2 system, the application should include a CCF assessment and plant safety~~qualitative~~ assessment ~~if the proposed design could introduce unanalyzed conditions due to the proposed implementation of combined design functions, shared resources, or connectivity to other plant systems. The basis for not performing a qualitative assessment should be documented~~ [You can't know this unless you perform the CCF assessment and plant safety assessment.].

[The only difference between these categories is that A1 should require deterministic defensive measures (e.g., diversity or testability) to reach a conclusion that CCF is prevented. A2 and B1 should permit qualitative defensive measures, including non-concurrent triggers.]

These criteria are 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." [These are the B2 systems.]

2.2. CCF Assessment Commensurate with Level of Integration and Interconnectivity

System integration and interconnectivity among the categories identified in Table 2-1 can introduce additional vulnerabilities to CCF. If there is integration (e.g., through combined design functions, shared resources, and/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 susceptibility to CCF of the integrated system and the consequences of CCFs that could affect the integrated or interconnected A1 systems [Why is this unique to A1 systems. Integration and interconnectivity also introduce potential CCFs that can adversely affect A2 and B1 systems; resulting in unanalyzed plant conditions.]. A D3 assessment should be performed in accordance with the guidance in Section B.3.1 on these interconnected or integrated systems to verify the design maintains defense-in-depth and meets applicable requirements [this statement is very ambiguous]. In performing this assessment, the criteria in Section B.3.1 for an A1 system apply to the interconnected or integrated systems. [To prevent CCF due to interconnections, A1 systems should require compliance to ISG-04 for communication independence and functional independence. Other independence methods could be defended for A2 and B1.]

If the licensee or applicant can demonstrate that existing or newly created interfaces or interconnections between A1 and systems in other categories do not have the potential to adversely impact the operation of the A1 systems (e.g., use of one-way digital communications output from the A1 system to systems in other categories rather than bi-directional communications) or reduce defense-in-depth, then the impacts of failures occurring within the non-A1 system(s) can be excluded from the D3 assessment for the A1 system. However, it is still necessary to ensure that CCFs occurring within or among the systems in the other categories do not result in the plant being put into a new unanalyzed state. See Section B.4 below for criteria on performing a qualitative assessment.

3. D3 Assessment

To defend against potential CCF, the NRC staff considers ~~three measures~~two steps to be key in the implementation of safety-related DI&C systems ~~that are safety significant (i.e., A1 systems)~~. These ~~three measures~~two steps are the performance of a ~~D3~~ CCF vulnerability assessment, which includes the use of defensive design measures to ~~avoid~~ prevent or tolerate faults, and a plant safety assessment which credits pre-planned actions and provisions to cope with unprevented CCFs to avoid unanticipated hazards or reactor conditions. The applicant or licensee should use the following criteria when performing a D3 assessment:

a. In accordance with Position 1 of the SRM on SECY-93-087, Item 18, II.Q, the licensee or applicant should perform a ~~D3~~ CCF vulnerability assessment. The CCF vulnerability~~D3~~ assessment should determine whether an A1 system is vulnerable to a CCF. Acceptable means that can be used to conclude there an A1 system is not vulnerable to a CCF, and thereby eliminate CCF from further consideration, are provided in Section B.3.1. If the means identified in Section B.3.1 are credited to eliminate the possibility of occurrence of CCF from further consideration for an A1 (or portions of an A1) system, then the D3 assessment will only need to identify and document the credited means and demonstrate the effectiveness of these means. In this case, items b. and c. (Positions 2 and 3 of the SRM on SECY-93-087, respectively) of this subsection would not apply to the A1 (or to portions of the A1) system under consideration.

b. In accordance with Position 2 of the SRM on SECY-93-087, Item 18, II.Q and the clarifications in SECY-18-0090, in performing the ~~D3~~ plant safety assessment, the licensee or applicant may use either best estimate methods (i.e., using realistic assumptions to analyze the plant response to DBEs) or conservative methods (i.e., design-basis analysis).

c. In accordance with Position 3 of the SRM on SECY-93-087, Item 18, II.Q, 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~~ plant safety assessment should identify the safety functions that are vulnerable to CCF and either 1) identify and document the diverse means that are credited for performing the same function or a different function; or 2) demonstrate that the consequences are within acceptable limits for each AOO or postulated accident within the safety analysis [but not with concurrent LOOP]. Section B.3.2 provides criteria for acceptable diverse means.

A ~~D3~~ CCF vulnerability assessment may credit one or more of the acceptable means identified in Sections B.3.1 and B.3.2 to address vulnerabilities to CCF. This includes crediting of appropriate preventive design features that prevent the occurrence of CCFs, as well as crediting appropriate design measures that limit ~~or mitigate~~ the effects of potential CCFs. [Mitigating a CCF is part of the plant safety assessment, not the CCF vulnerability assessment.]

~~When the Reactor Trip System (RTS) and ATWS mitigation system in an operating plant is modified, the~~The requirements of the ATWS rule, 10 CFR 50.62, must be met for new plants and upgrades to the RTS or ATWS mitigation system in operating plants. 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).

Acceptance Criteria [All of these sections entitled "Acceptance Criteria" simply repeat is in the guidance above them. This repetition makes the document much longer than it needs to be. All Acceptance Criteria sections should be deleted.]

The D3 assessment submitted by the licensee or applicant should demonstrate compliance with the NRC position on D3 described above. To reach a conclusion of acceptability, the following criteria should be met and supported by summation of the results of the assessment.

a. If any means as described in Section B.3.1 are credited to eliminate the credibility of a CCF affecting the A1 (or portions of the A1) system from further consideration, the acceptance criteria for use of the credited means have been met [I have no idea what this sentence is trying to say.]. In this case, items b. through e. of this subsection would not be applicable to the A1 (or portions of the A1) system.

b. If an A1 system is vulnerable to a CCF, then any of the diverse means provided in Sections B.3.2 can be used to address the CCF. The diverse means has been shown to:

    1. Be capable of responding with sufficient time available for the operators to determine the need for safety actions [this only applies where manual actions are credited; otherwise the automated system determines the need for safety actions] even with indicators that may be malfunctioning due to the CCF if credited in the D3 assessment;

    2. Be appropriate for the event;

    3. Be supported by sufficiently independent instrumentation that indicates:

        i. the safety function is needed,

        ii. the A1 system did not perform the safety function, and

iii. whether the automated diverse means or manual action is successful in performing the safety function [While this is nice to have it is not required, because there is no need to consider a failure of the diverse means concurrent with a CCF of the primary means.].

4. Ensure that the plant response calculated using realistic or conservative assumptions and analyses does not result in violation of the integrity of the primary coolant pressure boundary or radiation release exceeding ~~10 percent of~~ [this is not consistent with best estimate methods; meeting this was not required for previous BTP 7-19 reviews] the applicable siting dose guideline values.

If a diverse means is provided to perform the same or different function as the A1 system affected by the CCF, then items d. and e. below are not applicable.

c. No failure of non-safety related monitoring or display systems influence the functioning of an A1 system [This statement should be deleted. It is not related to CCF. Independence is a requirement of 603 and RG. 1.75.]. 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 has demonstrated that such operator-induced transients will be compensated by an A1 system function [This statement is not related to CCF; it should be deleted. A1 systems are demonstrated to be sufficient to mitigate AOOs and PAs; it is not the responsibility of the I&C designers to determine if the AOOs and PAs bound potential operator errors.].

d. For each AOO in the design basis occurring in conjunction with each single postulated CCF, the plant response calculated using realistic or conservative assumptions does not result in radiation release exceeding ~~10 percent of~~ [too conservative for a BDBE] the applicable siting dose guideline values or violation of the integrity of the primary coolant pressure boundary.

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

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

3.1. Means to Eliminate Further Consideration of CCF

Many system design and testing attributes, procedures, measures, and practices can contribute to significantly reducing the likelihood of CCF. However, there are certain design attributes that are sufficient to eliminate further consideration of ~~software-based or software-logic-based~~ a CCF due to a digital design defect. These attributes ~~include~~ are internal diversity and testability. If the licensee or applicant demonstrates that these design attributes of proposed DI&C systems

or components meet appropriate criteria, then a ~~CCF-induced malfunction analysis~~plant safety assessment does not need to be performed for those proposed systems or components. At least one of these attributes are needed to not perform a plant safety assessment for an A1 system, where a design defect can result in failure to perform its credited mitigation function. Other defensive measures may be credited to prevent CCFs for design defects that result in spurious operations in A1 systems, and for all design defects in A2 and B1 systems. Criteria for demonstrating that each of these design attributes are sufficient are provided in Sections B.3.1.1 and B.3.1.2 below.

Appropriate defensive measures can be used in the design of proposed A1 systems to prevent CCFs from occurring, or to limit or mitigate the consequences of CCFs. Criteria for demonstrating that design measures are sufficient are provided in Section B.3.1.3 below.

3.1.1. Use of Internal Diversity to Eliminate Further Consideration of CCF

If sufficient diversity exists within each safety division or among redundant ~~portions~~ divisions of an A1 system ~~to perform the safety function~~, then the potential for CCF ~~within these redundant portions~~ can be considered to be appropriately addressed without further action. The licensee or applicant should perform an analysis to demonstrate that sufficient diversity exists among these redundant portions of an A1 system such that they are not subject to the same CCF.

For example, a digital protection system could be designed such that each credited safety function is implemented in ~~two~~ a division~~s~~ that use one type of digital technology and another ~~two~~ division~~s~~ that use a different digital technology [there is no regulatory requirement for four divisions]. An analysis should be performed to demonstrate that the diversity attributes among the redundant portions of the A1 system are adequate to assure that the two diverse portions of the A1 system are not subject to the same sources of CCF. If this can be demonstrated, no additional diversity would be necessary in the safety system.

However, it should be noted that since each redundant safety division is credited for compliance to the single failure criteria and is now additionally credited to prevent CCF, the technical specification bypass times and completion times are likely to be more restrictive than if the redundancy is only credited for single failure compliance.

Acceptance Criteria

To reach a conclusion that no additional diversity is needed for the proposed design, the following criteria should be met:

a. Each safety function to be achieved by the proposed design is shown to be independently achievable by each ~~different technology~~diverse design[4] used in the system. [This BTP should not imply that acceptable diversity can only be achieved using different technology.]

[4] Different diversity attributes could be used to demonstrate that the diverse portions within the proposed design can achieve the credited safety functions independently. Different technology is one such diversity attribute.

b. The ~~systems (redundant~~ diverse portions~~)~~ of the system do not have common or shared resources, such as power supplies, memory, bus or communications modules, which could have a digital design defect that could defect both diverse designs, nor do the ~~different technologies~~ diverse designs employed share ~~configuration~~ engineering or maintenance tools, which could become a source of common cause vulnerability.

c. Each ~~different technology~~diverse design 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.

d. Periodic surveillance criteria are used to verify the continued operability of each ~~channel~~diverse design.

3.1.2. Use of Testing to Eliminate Further Consideration of CCF

When considering potential sources for software CCF, there are two general areas of concern – ~~(1) CCF as a result of errors introduced by the design requirements or specifications; [again if you introduce this you no longer distinguish digital from analog]~~ and (2) CCF as a result of errors introduced during the design implementation of the digital hardware, software or software-based logic. A quality design process ~~may be~~has always been credited to address potential errors in the design requirements or specifications. Testing may be credited as a means to address potential CCFs in a digital device or component as a result of potential latent defects in the design, fabrication, ~~and~~ or implementation of software or software-based logic.

To credit testing as a means of demonstrating potential design, fabrication, and implementation errors have been identified and corrected such that the device and component will function as specified under all conditions, the licensee or applicant should meet the criteria below:

a. The combination of every possible input is included in the testing. Given this input is for a digital device or component, the input should be digital [I think you are saying that this testing method cannot apply to systems/components with analog inputs; but this is not clear. This would preclude testing as a CCF preventive measure for most applications, because most applications have analog inputs. Analog inputs can have an infinite number of states and those states can change in any direction and with any frequency. They certainly make testing very difficult. You need to clarify your point.]. Any unused input that ~~are~~ is permanently forced to a fixed state ~~does not need to be included~~can be at that fixed state during ~~in~~ this testing.

b. Where 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 ~~of these inputs~~ in the testing.

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 all possible past condition sequences should ~~either be shown to not impact the device output or~~ [how can you do this without testing] be included in the testing.

d. If a device or component includes logic or circuits that are not used under any

operational condition, and 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, then it is possible that that logic or circuitry might be excludable from the testing ~~without resulting in a need for D3 assessment~~ [this is part of the CCF vulnerability assessment].

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. These testing provisions are intended for application to devices and components that are simple enough for such testing to be practical.

Acceptance Criteria

To reach a conclusion that sufficient testing has been performed on a device or component such that CCF can be eliminated from further consideration, the following criteria should be met: [Change the sections below for consistency with the markups above.]

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

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

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 shown to either not impact the device output or be included in the testing.

d. If a device or component includes logic or circuits that are not used under any operational condition, the unused logic or circuitry has been shown to 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 Other Defensive Measures to Eliminate Further Consideration of CCF [diversity and testing are defensive measures]

In addition to the use of internal diversity or testing, there may be other defensive measures that are effective to prevent~~, limit, or mitigate the effects of~~ [limiting and mitigating does not eliminate CCFs from further consideration] a potential CCF in A2 and B1 ~~a~~ DI&C systems. If a licensee or applicant credits the use of such defensive measures to eliminate potential CCFs from further consideration, the following criteria should be documented:

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

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

c. A description of how the potential CCF hazard will be prevented, limited, or mitigated by the proposed design 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 postulated CCF are limited, mitigated or prevented. This includes an analysis of how the effectiveness of the measures credited can be demonstrated

e. An assessment of any residual risks from potential CCFs

If a licensee or applicant uses defensive measures as the only credited means to address potential CCFs in a DI&C system, the defensive measures being credited, along with a supporting technical basis and acceptance criteria should be based upon an NRC-approved methodology [what does this mean; there is no NRC-approved methodology].

Acceptance Criteria

The credited defensive measures to ~~address~~ prevent CCF in an A2 or B1 DI&C system or component along with the documented supporting technical basis and acceptance criteria, are based upon an NRC-approved methodology [what does this mean; there is no NRC-approved methodology].

3.2. Use of Diverse Means to Address CCFs

Per Position 3 of the SRM on SECY-93-087, Item 18, II.Q, a diverse mean should be provided to accomplish the same or different function than the safety function disabled by the postulated CCF. Sections B.3.2.1 through B.3.2.3 provide acceptable diverse means to meet Position 3 of the SRM on SECY-93-087, Item 18, II.Q. If the CCF vulnerability assessment finds no CCF vulnerabilities, then a diverse means is not required.

3.2.1. Crediting Existing Systems [I see no need for this document to distinguish existing systems from new systems. The only requirement is that the credited system be diverse and of suitable quality, regardless of new or existing. If you leave this section you should also include existing control systems which are often credited for SBLOCA and AOOs where the control system is not the initiator. Control systems may not have augmented quality, but are in continuous use.]

As a means of addressing CCF of an A1 system, an existing ~~high reliability~~ [only high quality is required by SECY 93-087; this was referred to augmented quality. High reliability implies redundancy, which is not required for credited diverse equipment. In the past the staff has also accepted crediting systems that are in continuous use, such as control systems, because their failure is immediately self-announcing.] I&C system can be used to perform same safety function or a different function from the intended safety function disabled by a postulated CCF. The function performed by this ~~high reliability~~ I&C system should result in plant consequences that do not exceed the limits prescribed for each AOO or postulated accident in the final safety analysis report [This is not correct. Since CCF due to a design defect is a BDBE, limits are based on offsite radiation limits, RCS integrity and containment integrity, not the current limits in

the FSAR transient and accident analysis (TAA)]. 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 is not subject to the same postulated CCF. Section 2.6, "Diversity," of NUREG/CR-6303 identifies six diversity attributes and 25 related diversity criteria that can be used to support this qualitative analysis.

The existing system may be a system that is not safety-related provided it is of sufficient quality and can reliably perform the required functions under the associated event conditions. 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 digital system. The ATWS system to be credited should 1) be ~~independent of~~diverse from the proposed DI&C system [there is no requirement for independence to address CCF]; 2) has been demonstrated to be highly reliable; and 3) be responsive to the AOO or postulated accident event sequences ~~using independent sensors and actuators~~ [While the ATWS system requires independent actuators for diverse RT, it does not require independent sensors. Neither are required to be independent for compliance to SECY 93-087. The only requirement is that there be no common design defect with the primary safety system that could result in a CCF of both.] as the proposed DI&C system.

Acceptance Criteria

To reach a conclusion of acceptability of crediting an existing plant system as the diverse means used to perform the same or different function as the proposed DI&C system, the following criteria should be met:

a. The equipment to be credited is highly reliable 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; or 2) is capable of sensing and responding to alternative plant conditions that are expected to occur as a consequence of the AOO or postulated accident. ~~For both these options, the capabilities for sensing and responding have been shown to meet the response time requirements of the proposed DI&C system for each AOO or postulated accident in SAR~~[This implies that the diverse system must meet the same response time requirements as the primary protection system. This is not correct because CCF is a BDBE with relaxed initial conditions and relaxed acceptance criteria. Therefore, the diverse system can have much slower response time.].

d. The equipment to be credited has the required functional characteristics necessary to ~~maintain the plant within the accepted limits~~ meet the relaxed acceptance criteria for BDBEs.

[Need to allow crediting systems that do not have augmented quality but are in continuous use.]

3.2.2. Crediting Manual Operator Actions

Manual operator actions can be used as a diverse means to provide the same or diverse function credited in the D3 assessment. If manual operator actions are used as the diverse means, the equipment necessary to perform these actions, including the supporting indications should be diverse and independent from the ~~automatic~~ [manual actions may be credited in the TAA] safety-related I&C system credited in the TAA and disabled by a potential CCF. 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~~ hot shutdown condition [The SRP Section 7 defines safe shutdown as cold shutdown. But in the past the staff has accepted achieving and maintaining hot shutdown until the CCF in the primary safety system has been corrected. Thereby allowing a transition to cold shutdown using the primary safety system. Achieving and maintaining cold shutdown requires diverse equipment for many more functions and components.]. A CCF that affects normal displays or controls should not prevent the operator from manually ~~initiating~~ controlling critical safety functions. [Initiating safety functions requires the diverse equipment to have the same capabilities as the primary safety system. Controlling critical safety functions is all that is required by Position 4 of SECY 93-087.]

The licensee and applicant should perform a Human Factors Engineering (HFE) analysis to demonstrate that ~~plant conditions can be maintained within recommended acceptance criteria for the particular~~ [maintaining plant conditions requires a safety analysis, which is much more than an HFE analysis] manual actions credited in the plant safety assessment for mitigating an AOO or postulated accident with concurrent CCF can be taken reliably. The credited manual operator actions and the equipment necessary to perform these actions should be identified. If equipment outside of the MCR is used to perform these actions, then the reliability, availability, and accessibility of the equipment under the postulated event conditions should be demonstrated. It is noted that while equipment outside the MCR can be credited for AOO or PA mitigation, Position 4 requires controls for all critical safety functions in the MCR. 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

To reach a conclusion of acceptability of manual operator actions as the diverse means used to perform the same or different function as the automatic DI&C system, the following criteria should be met:

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

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

c. The HFE analysis demonstrates the acceptance criteria provided in Appendix 18-A of SRP Chapter 18, “Crediting Manual Operator Actions in Diversity and Defense-in-Depth Analyses” have been met.

Note: The difference between Time Available (as determined by the thermal hydraulic analysis) and Time Required (as determined by the HFE analysis) for operator action 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 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.

3.2.3. Crediting a Diverse Actuation System

A~~n automated~~ diverse system (e.g., diverse actuation system), including automated and/or manual functions [a DAS typically includes both, as needed for BDBE mitigation], could be credited as a diverse means to address CCF. If such a~~n automated~~ system is credited as a diverse means to address CCF, the licensee or applicant should demonstrate that 1) the functions performed by this ~~automated~~ diverse means are adequate to maintain plant conditions within recommended acceptance criteria for the particular BDBE; and 2) sufficient diversity exists between this ~~automated~~ diverse means and the A1 system subject to the CCF. An analysis should be performed to demonstrate that the ~~automated~~ diverse means to be credited and the digital design used for the proposed A1 system is not subject to the same postulated CCF. Section 2.6, "Diversity," of NUREG/CR-6303 identifies six diversity attributes and 25 related diversity criteria that can be used to support this qualitative analysis.

The ~~automated~~ diverse means may be performed by a system that is not safety-related, 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 reactor coolant system inventory control system or normal steam generator level control system) are not required to be upgraded to the augmented quality discussed above [this section is about DAS; this sentence about continuous use control system is important, but it needs to go in the section above as previously commented].

Prioritization between safety-related systems and the diverse system that is not safety-related to ensure the credited safety function can be accomplished by either system is addressed as follows:

a. ~~Safety-related c~~ [You cannot give priority to safety-related commands, because a CCF can result in erroneous safety-related commands that would keep the diverse system from putting the component in the safe state. For the same reason you cannot give priority to the diverse commands. This is why there must be state-based priority, not system-based priority.] Commands, auto or manual and from either the primary or diverse system, that direct a component to a safe state must always have the highest priority and must override all other commands. If the component has two safe states, then priority should be given to the state that is not the normal state of the component and an alarm should be provided if the component transitions to that state during normal operation. For example, emergency feedwater isolation valves are normally open. The

open state is needed to feed an intact steam generator on a low water level condition. But those valves are closed to isolate a ruptured steam generator. Both are safe states for different accidents. By giving the close state highest priority, either the primary or the diverse system can close the normally open valves when needed for accident mitigation. If those valves are closed for any reason during normal plant operation, including a valid signal or a spurious operation, an alarm is generated (e.g., BISI alarm) to ensure the valves are promptly returned to their normally open state. With this alarm, it is reasonable to conclude that the valve will be returned to its normally open position prior to an accident that would require that safe state.

b. Commands that originate in a safety-related ~~channel~~ system [introducing channel adds confusion] 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. [This sentence is not understandable. I see no need for it; the priority defined in (a) is sufficient.]

c. The reasoning 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. [This should reference ISG-04 which includes many very important requirements for digital priority logic functions, including non-volatile unalterable memory that cannot be changed unless the equipment that contains the priority logic is physically removed from the system.]

Acceptance Criteria

To reach a conclusion of acceptability of a diverse ~~automated~~ system for providing the diverse means to perform the same or different function as the ~~A1~~ primary safety [there is no reason to limit this to A1; diverse systems can also be applied for A2 systems.] system, the following criteria should be met:

a. The functions performed by this diverse ~~automated~~ system are adequate to maintain plant conditions within the accepted limits for the particular BDBE.

b. Sufficient diversity exists between this diverse ~~automated~~ system and the ~~A1~~ safety system subject to the CCF.

c. The equipment to be credited has the required functional characteristics necessary to maintain the plant within the accepted limits.

d. Any use of priority functions to prioritize between the diverse ~~automated~~ system and the ~~A1~~ safety system (or other systems/manual operator actions) 1) ensures that the ~~safety-related~~ commands that direct a component to a safe state ~~has~~ have the highest priority, and 2) the documented basis for the priority ranking is appropriate.

e. If equipment that is not safety-related is used in the automated system, the equipment is

highly reliable and is expected to be available during the associated event conditions.

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 a structure, system, and component (SSC) with digital technology, referred to as a qualitative assessment. The qualitative assessment, as described in Supplement 1 of RIS 2002-22, is intended for modifications to SSCs of low safety significance (i.e., A2 and B1) and not high safety significant systems (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), consistent with the updated final SAR or final SAR analysis assumptions for the proposed DI&C system. These three factors include:

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

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

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

Consideration of these three factors as well as supporting failure analysis information also described in RIS 2002-22, Supplement 1, is an acceptable method to address potential CCF vulnerabilities, which provide reasonable assurance of safety for systems of lower safety significance. The licensee or applicant should perform a qualitative assessment that documents 1) how these three factors have been used to reduce the likelihood of a CCF to eliminate it from further consideration; and 2) the supporting failure analysis. [What you are describing is the same CCF vulnerability analysis required for A1 systems. The only difference is that to reach a CCF prevented conclusion (or 'CCF requires not further consideration conclusion') you are permitting qualitative attributes for A2 and B1 and only deterministic attributes (i.e., testing and internal diversity) for A1. Therefore, you could simplify this entire document by stating that all three categories require a CCF vulnerability assessment followed by a plant safety assessment for any CCFs that are not prevented. The only difference is in the attributes that can be credited to reach a CCF prevented conclusion.

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 is referred to as "sufficiently low." The concept of sufficiently low was developed to address the likelihood of a CCF of a system modified with digital technology, ~~specifically CCF due latent defects in the software or software-based logic of a DI&C system~~[this is not correct. The RIS also addresses single failures. For example, "if previously separate functions are combined in a single digital device, the failure analysis should consider whether single failures that could previously have affected only individual design functions can now affect multiple design functions.". The sufficiently low definition incorporates consideration of failure likelihood of a proposed SSC to failures documented in the FSAR. This approach can also be used for a new

reactor design, where by the likelihood of failure of a DI&C system should be aligned with the assumptions in the FSAR.

To reach a conclusion of acceptability, the following criteria should be met and supported by summation of the results of the qualitative assessment.

a. Design attributes and features have been implemented and shown to provide reasonable assurance of effectiveness for reducing the likelihood of potential CCFs such that their occurrence is sufficiently low.

b. Quality of the design process of the DI&C system provides reasonable assurance the potential for CCFs due to latent defects in the software or software-based logic in the DI&C system are sufficiently low.

c. Any applicable operating experience regarding the DI&C system have been evaluated to provide reasonable assurance that the DI&C system will operate with high reliability for the intended application.

[Now you need to explain what is required if "sufficiently low" is not achieved (i.e., a plant safety assessment is required).]

5. Spurious Operation

The potential for CCFs in DI&C systems to cause spurious operation of ~~a~~ multiple safety or non-safety functions [if only a single function is affected, it is not a CCF] that could place the plant in an unanalyzed condition or challenge plant safety should be evaluated. In ~~many~~ some cases, these spurious operations are already identified in a plant's safety analysis. ~~, or are bounded by the events already addressed in the safety analysis.~~ [first discuss the CCF vulnerability assessment, then the plant safety assessment later.] However, some spurious operations due to integration and/or interconnectivity of DI&C systems have not been considered in the safety analysis. ~~, and thus may lead to unanalyzed or unbounded plant conditions.~~ For example, multiple functions can be combined into a single DI&C system, which increases the potential for spurious actuations of multiple functions. This integration may be introduced within a single digital controller that controls multiple functions that were previously controlled by separate devices, between multiple controllers that share a common resource, such as a digital data communication interface or ~~at the~~ a human ~~machine~~ systems interface (for consistency with NUREG-0700 and 0711) where an operator can control multiple safety components, multiple ~~and~~ non-safety components or multiple safety and non-safety components, using a single control and display workstation. For new spurious operations, not previously identified in the plant's safety analysis, it may be possible to demonstrate through the plant safety assessment that they are bounded by the events already addressed in the safety analysis. If not, new safety analyses may be needed.

A spurious operation due to a CCF originating ~~in the software or software-based logic of a~~due to a design defect in a DI&C system ~~is~~ can be considered beyond design basis for systems that have a robust design process, because the likelihood of a design defect is low. Assessing a robust design process may include a graded approach depending on the system's safety significance. For example, compliance to commercial standards for high quality design processes, such as ISO-XXXX, with supplemental V&V at the application level, would be sufficient to conclude that a design defect is beyond design basis. For new spurious operations,

not identified in the plant's TAA, the plant safety assessment may use "best-estimate" methods and acceptance criteria as previously described. Even if new spurious operations are not bounded by the current AOOs or PAs in the plant's TAA, they do not need to be added to the TAA because they are BDBEs.

However, a spurious operation due to a ~~random~~ single failure~~s (e.g., random hardware failure) are~~ is within the design basis, because single failures are expected during the life of the plant. Single failures in safety systems (A1 and A2) ~~and should be~~are addressed by the single failure criterion, which requires consideration of electrical faults and external hazards (e.g., flood, fire). Single failures in non-safety systems (B1) may be limited to random hardware failures. For new spurious operations that are within the design basis, the plant safety assessment must use conservative methods and acceptance criteria (i.e., the same methods and acceptance criteria as in the plant's TAA). If new spurious operations are not bounded by the current AOOs in the plant's TAA, they must be added to the TAA because they are new AOOs (i.e., expected during the life of the plant).

The licensee or applicant should perform an analysis to identify spurious operations due to CCF of a DI&C system. For any CCFs that are not prevented, a plant safety assessment should be conducted to identify any spurious operations that ~~has the potential to~~ lead to unanalyzed or unbounded conditions. The following criteria should be met to analyze ~~for potential~~ [the bullets below (except c) are for the safety assessment (i.e., CCFs not prevented), not the CCF vulnerability assessment] spurious operations from DI&C systems:

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

b. Spurious operations considered within the safety analysis should remain bounded given a postulated CCF of the DI&C system performing the actuation functions. Unbounded CCFs should be addressed as described above (i.e., either new AOOs or BDBEs)

c. Design attributes or defensive measures can be credited in the spurious operation analysis to eliminate from further consideration of a CCF of a DI&C system. If any such design attributes or defensive measures are credited, the design attribute should be identified, and its effectiveness should be demonstrated with reasonable assurance. Section B.3.1 provides criteria on the use of design attributes and defensive measures to eliminate CCF from further consideration.

d. The analysis should focus on those functions whose spurious operation can create ~~an unbounded condition in the safety analysis unless mitigated by another automatic system or manual operator actions~~plant transients [you don't know if they are unbounded or can be mitigated until you do the transient analysis.].

    1. Section B.3.2 provides criteria on the use of automatic functions and manual operator actions.

    2. The analysis to demonstrate that potential spurious operations are bounded by the safety analyses and can be qualitative or quantitative depending on the design basis or beyond design basis source of the CCF.

3. If ~~quantitative~~ qualitative analysis is performed to evaluate the consequence of a potential CCF, either best estimate methods or conservative analysis methods may be used. [Best estimate methods cannot be used if a quantitative analysis is required for a DBE.]

e. In cases where the credited design attributes or defensive measures cannot provide reasonable assurance that the potential for spurious operation due to a CCF in the DI&C system, the following criteria should be used to perform the plant safety ~~analysis~~assessment [the three items above also address this situation.]:

1. The quality development process of a safety-related DI&C system may be credited to reduce the likelihood of CCFs that could lead to spurious operation ~~of a safety function~~ [this section is for both safety and non-safety systems]. As such, only spurious operation of a single ~~safety~~ function (e.g., spurious actuation of both emergency core cooling system trains) needs to be considered at a time when performing this analysis [this is not correct. First – with sufficient diversity non-concurrent triggers and self-announcing can be credited such that a design defect is triggered in only one controller, then corrected in all controllers; therefore, the event is limited to a single controller in a single train. Second – within one controller the design defect may adversely affect multiple functions, not just one function. For example, a defect in a function block will adversely affect all applications that use that same function block (e.g., a defect in a 2oo4 voting block may cause spurious operation of all ESF functions; a defect in a PID block may cause spurious operation of multiple control functions that use that PID function block.].

2. For discrete [what is a discrete system; this is not defined] digital control systems (i.e., a system that performs only a single control function, such as feedwater control), only potential spurious operation of the components controlled ~~functions performed~~ by this single system need to be considered when performing this CCF analysis. If only one component is controlled by a controller, then there is no potential for a CCF due to a single random failure. If there is sufficient diversity among different controllers (e.g., application level diversity), then a CCF of multiple controllers due to a design defect can be precluded based on non-concurrent triggers. Therefore, failure of a discrete controller is likely to be already considered in the TAA.

3. For highly-integrated DI&C systems ~~that is not safety-related~~ [this is not limited to non-safety systems](e.g., distributed control systems), the analysis should demonstrate that potential spurious operation of multiple functions/components is still bounded by the safety analysis, or new DBEs should be added to the TAA.

4. The analysis should include evaluation of potential spurious operation of multiple safety-related components or components that are not safety-related (or both) from the use of ~~multi-divisional~~ control and display stations to control these components [even VDUs that control only a single division can cause spurious operation of multiple components within that single division; this is a CCF.].

Acceptance Criteria

The results of the analysis should include a documented evaluation that provides reasonable assurance to demonstrate that:

a. Spurious operations currently evaluated in the safety analysis remain bounded given an ~~postulated~~ unprevented CCF within the DI&C system [It is very important that there is no requirement to postulate a CCF. The CCF vulnerability analysis determines if a CCF is credible or prevented.].

b. Measures implemented to prevent or limit the consequence of potential spurious operations are adequate.

c. Means used to mitigate the consequence of the spurious operation (e.g., crediting another automatic system or use of manual operator actions) are adequate and these means are unaffected by the CCF of the DI&C system. If manual operator actions are credited, then the availability of indications for the operator to recognize that a spurious operation has occurred and sufficient time for the operator to perform the credited manual operator actions.

6. Manual System Level Actuation and Indications

Displays and manual controls provided for compliance with Position 4 of the SRM on SECY-093-87, Item 18, II.Q 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 [No, the SECY does not require achieving safety shutdown with Position 4 controls; it only requires controlling critical safety functions.]. For DI&C system modifications to operating plants, retention of existing analog displays and controls in the MCR could satisfy this position. However, if existing displays and controls are digital and/or the same platform is used to for accident mitigation and to provide signals to these analog displays, this position may not be satisfied.

Once ~~system-level manual actuation~~critical safety functions have been controlled and stabilized 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. [It is not sufficient to just actuate safety functions from the MCR; this is not the intent of the SECY.]

The following criteria should be met for these displays and manual controls:

a. 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.

b. The indications and manual controls ~~for these~~to return these critical safety functions to acceptable stable conditions or maintain them at acceptable stable conditions should be at the system-level and located within the MCR.

c. Safety-related equipment or equipment that is not safety-related can be used for these indications and manual controls and indications.

d. The displays and controls should be ~~independent and~~ [independence implies they cannot be within the same division; this is not correct.] diverse from the safety-related DI&C systems such that these display and controls are not affected by potential CCFs that could disable ~~automatic~~ the safety-related DI&C systems that are normally credited for AOO/PA mitigation.

e. The displays may include digital components provided that they cannot be adversely affected by a CCF of the safety-related DI&C systems.

Acceptance Criteria

To reach a conclusion of acceptability of the manual controls and supporting indications to meet Position 4 of the SRM on SECY-93-087, Item 18 II.Q, the licensee or applicant should demonstrate 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 and located within the MCR. Since single failures concurrent with a CCF are not required to be postulated and normal alignment of equipment is assumed, the capability for manual actuation of a single division is sufficient [this is true for all diverse functions, so it should be added in sections that address systems credited for Positions 2 and 3 also. However, it should be noted that if only one division is provided, then bypass times and completion times for that division will be more restrictive than if redundancy through two divisions is provided.]. For plants licensed to allow one division to be continuously out of service, the diverse manual actuation applies to at least one division that is in service.

c. If equipment that is not safety-related is used, the quality of the equipment is adequate to support the manual operator actions during the associated event condition or the equipment is in continuous use.

d. The displays and controls are ~~independent and~~ diverse from the safety-related DI&C systems such that these display and controls are not affected by potential CCFs that could disable ~~automatic~~ safety-related DI&C systems. ~~If the displays and controls contain digital components, they are shown to not be adversely affected by a CCF of the safety-related DI&C systems~~[this just repeats the sentence above].

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 DI&C system and the supporting technical basis for this categorization.

b. For an A1 system [the same review is required for A2 and B1 systems] , the D3 assessment of the A1 system, which includes:

   1. Identification of any credited design attribute or defensive measure to eliminate CCF from further consideration and demonstration that these attributes or measures are effective. Identification of any remaining vulnerabilities to potential CCFs. To preclude a CCF due to a design defect in A1 systems diversity or testability is required. For A2 and B1 systems other design attributes can be defended. To prevent a CCF due to single failures, the single failures for A1 and A2 systems must encompass the failures identified in the single failure criteria of IEEE-379. For B1 systems the single failures are limited to random hardware failures.

   2. For CCFs that result in failure to actuate that are not prevented, Identification of any diverse means provided to accomplish the same or different function than the safety function disabled by a potential CCF. If any diverse means are credited to address the potential CCF, the staff should review the information provided to demonstrate the effectiveness of the diverse means, including any HFE analysis associated with manual operator actions as a diverse means.

   3. Identification of any analysis performed to demonstrate that consequences due to a potential CCF is within acceptable radiological release limits. If any consequence analysis has been performed, the staff should review the results of this analysis.

c. For A2 and B1 systems, the qualitative assessment of these systems, which includes information: [I see no need for this qualitative assessment distinction. The only difference between A1 and A2/B1 systems is the defensive measures that can be credited to prevent a CCF.

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

   2. Regarding the quality of the design and development process to support potential for CCFs due to latent defects in the software or software-based logic of the system.

   3. Regarding applicable operating experience to provide reasonable assurance that the DI&C system will operate with high reliability for the intended application.

d. For ~~a~~ A1, A2 and B2 systems, information provided to show that the proposed design will not introduce any unanalyzed conditions due to the specific implementation [Spurious operations in A1, A2 or B2 systems can result in unanalyzed conditions.].

e. Results of the spurious operation analysis to verify either:

1. The consequence of a potential spurious operation due to a CCF is bounded by the plant safety analysis; or

2. Vulnerabilities to potential spurious operations due to a CCF have been addressed through use of design attributes or defensive measures to prevent, limit or mitigate the consequence of a CCF.

f. For an unprevented ~~proposed~~ CCF in an A1 system, design information provided to verify that controls and displays:

1. have been provided in the MCR to ~~perform manual system level actuation of~~restore or and/or maintain critical safety functions;

2. are not subject to the same CCF that could disable the ~~safety function~~A1 system; and

3. have adequate quality to support the manual operator actions during the associated event condition if the equipment used are not safety-related.

8. Review Procedures

In reviewing the licensee or applicant's ~~D3~~ CCF vulnerability assessment and plant safety assessment using the acceptance criteria described in Section 3 of this BTP and the detailed guidance of NUREG/CR-6303, emphasis should be given to the following topics:

8.1. System Representation as Blocks

The system being assessed is represented as a block diagram; the inner workings of the blocks are not necessarily shown. Diversity is determined at the block level. A block is a physical subset of equipment ~~and~~ or 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 PID block, that is used by multiple functional applications; a design defect in this type of block can result in a CCF of all application functions that utilize that block.

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

8.2. Documentation of Assumptions

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.

8.3. 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.

8.4. Effect of Other Blocks

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

8.5. Identification of Alternate Trip or Initiation Sequences

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.) [Also requires a review by HFE experts for any diverse credited manual actions.]

8.6. 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 in an automatic or manual function credited in the TAA 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 adequate information (indication), appropriate operator training, and sufficient time for operator action are available in accordance with Appendix 18-A of SRP Chapter 18.

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

8.7. Justification for Not Correcting Specific Vulnerabilities[5]

If any identified vulnerabilities are not addressed by design modification, refined analyses, or provision of alternate trip, initiation, or mitigation capability, justification should be provided.

[5] Work in this section is still on-going.

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 279-1971, “Criteria for Protection Systems for Nuclear Power Generating Stations,” Piscataway, NJ.

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

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

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

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

7. 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.

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

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

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

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

12. U.S. Nuclear Regulatory Commission, “Manual Initiation of Protective Actions,” Regulatory Guide 1.62.

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

14. 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.

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

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

17. 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 information will be provided in the final version of this document.

PUBLIC PROTECTION NOTIFICATION

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

BTP Section 7-19

Description of Changes

BTP 7-19, "GUIDANCE FOR EVALUATION OF POTENTIAL COMMON CAUSE FAILURE IN DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS"

This BTP section updates the guidance previously provided in Revision 7, dated August 2016. See ADAMS Accession No. ML16019A344.

The main purpose of this update is to provide clarification on sections of the guidance that proved challenging to implement based upon feedback received by internal and external stakeholders. This update improves readability and the flow of information such that it is clear to the reader that there is an established process for analyzing for potential hazards caused by CCF of digital technology, in particular within software. 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 is consistently applied. This is in addition to clarifying specific areas of guidance such as with regard to diversity and testing to eliminate further consideration of CCF. 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 which correlates to the graded approach methodology.