APPENDIX E

Analysis of Public Comments on Branch Technical Position 7-19, “Guidance for Evaluation of Common Cause Failure Hazards due to Latent Design Defects in Digital Instrumentation and Control Systems”

Comments on the subject draft branch technical position (BTP) are available electronically at the U.S. Nuclear Regulatory Commission’s (NRC’s) electronic reading room at http://www.nrc.gov/reading-rm/adams.html. From this page, the public can access the Agencywide Documents Access and Management System (ADAMS), which provides text and image files of the NRC’s public documents. The following table lists the comments the NRC received on the draft BTP.

Letter Number	ADAMS Accession No.	Commenter Affiliation	Commenter Name
1	ML20030A108	Member of the Public	Thomas Gurdziel
2	ML20036F116	Nuclear Automation Engineering, LLC (NAE)	Ken Scarola
3	ML20041D903	SunPort	Mark Burzynski
4	ML20041D907	SunPort	Mark Burzynski
5	ML20054B246	SunPort	Mark Burzynski
6	ML20054B264	Member of the Public	Yi Yu
7*	ML20077L523	NAE	Ken Scarola
8	ML20080G707	Nuclear Energy Institute	NEI

* Note: Letter 7 provided comments responding to comments in Letter 4. The NRC staff will address Letter 7 comments in the staff’s responses to Letter 4 comments.

This document lists each public comment by letter number, as listed in the table above. The original comment, as written by the commenter, is provided first, followed by the NRC’s response.

Letter 1—Comments from Mr. Gurdziel

Comment No. 1-1

I have just read through all 32 pages of Branch Technical Position 7-19, Rev 8. It is apparent to me that a lot of very serious thinking has gone into this guidance document and I find that very impressive. However, there is something missing, (at least in my mind.) All items in Section C, References, come only from the United States. Why is that?

I would like to see that this guidance document takes advantage of the knowledge and perhaps experience of at least five other nuclear plant regulators who have, (or may have), addressed the Digital Instrumentation & Control Common Cause Failure problem in their nuclear fleets. Those five would be, first: France. Next: China. Next: South Korea. Next: Russia. Next: Canada.

It is my understanding that France is currently on their 4th generation of digital I&C. We, here in the USA, aren't even on our 1st!

NRC Staff Response

The NRC staff agrees with the comment that it is important to consider the experience of international regulators. However, the NRC staff did not change Section C, “References,” of the Branch Technical Position (BTP) 7-19, since the references in Section C already take into account such international experience. For example, BTP 7-19 references NUREG/CR-7007, “Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems,” which refers to guidance from several international standards, including International Atomic Energy Agency (IAEA) S-G-1.3, “Radiation Aspects of Design for Nuclear Power Plants,” International Electrotechnical Commission (IEC) 62340, “Instrumentation and Control Systems Important to Safety—Requirements to Cope with Common Cause Failure (CCF),” IEC 60880, “Nuclear Power Plants—Instrumentation and Control Systems Important to Safety—Software Aspects for Computer-Based Systems Performing Category A Functions,” and IEC 61511, “Functional Safety: Safety Instrumented Systems for the Process Sector.”

Even though the staff did not modify the document as a result of this comment, the NRC staff continues to engage with international regulators on topics such as DI&C. For example, the NRC staff engages, through the Nuclear Energy Agency, with experts from the countries noted in the comment, along with many others, to develop documents such as the “Common Position on the Treatment of Common Cause Failure Caused by Software within Digital Safety Systems.” (Reference: OECD-NEA, MDEP Generic Common Position No. DICWG-01, dated June 17, 2013). In addition, NRC staff members regularly participate in international bilateral meetings with representatives of international regulatory bodies during which digital I&C regulatory practices are discussed and compared. This BTP is consistent with the international common position.

France has updated its I&C systems using digital technology multiple times. In US nuclear power plants (NPPs), digital I&C technology has been in use in critical functions since the early 1980s. Further, several US NPPs have already upgraded their digital controls and indication systems to newer generations over the years, as needed.

The criteria in BTP 7-19 are primarily based on criteria referenced in Institute of Electrical and Electronics Engineers (IEEE) Stds. 279-1971 and 603-1991, which are incorporated by reference in Title 10 of the Code of Federal Regulations (10 CFR), Section 50.55a(h), and apply to many U.S. nuclear power plants. Nonetheless, as described above, the NRC staff has considered the knowledge and experience of international regulators when developing Revision 8 of this BTP.

Letter 2—Comments from NAE

Note: Within the Letter 2 submittal, the commenter provided suggested edits to draft BTP 7-19, Revision 8, for the NRC staff’s consideration. The NRC staff contacted the commenter and confirmed that the commenter is not requesting a resolution to the suggested edits but rather that the edits be used as supplemental information to resolve the comments.

Comment No. 2-1

The title of this BTP, the Purpose section and most other sections throughout this BTP put undue emphasize on CCF due to a software defect; it is important to equally emphasize other *sources of CCF that apply to digital systems (due to its complexity), that did not apply to its analog predecessors.*

Computer industry experience, including the defects recently discovered in the 737 Max, demonstrate that a system design defect, which encompasses both digital hardware and software, is much higher likelihood than a defect in software alone. There are a few sections in this BTP (A, B.1.1, B.1.3, B.3.1.2, and B.4) that correctly state that defects in system design, hardware or system components can lead to a CCF; but all sections that provide guidance on addressing CCF refer only to software defects. Most importantly, even though a CCF due to a random failure in a shared hardware resource (e.g., processors, networks) is significantly more likely to occur than a CCF due to any design defect, making it a design basis event (DBE) compared to a beyond design basis event (BDBE) for a design defect, Section A.4 is the only section that mentions CCFs due to a random hardware failure, and no guidance or acceptance criteria are provided to address it; the current statement regarding RG 1.53 is incorrect, because RG 1.53 does not provide guidance for addressing a single random hardware failure that leads to a CCF of multiple safety or non-safety plant functions or plant components.

10 CFR 50 Appendix A General Design Criteria requires "Consideration of the possibility of systematic, nonrandom, concurrent failures of redundant elements in the design of protection systems and reactivity control systems. (See Criteria 22, 24, 26, and 29.)" SECY 93-087 was written to address new sources of CCF that apply to digital systems that did not apply to analog systems; SECY 93-087 does not limit the new sources of CCF to a software defect. Shared hardware resources are identified in the very first paragraph of SECY 93-087 as potential sources of CCF; hardware design error is identified in the second paragraph. To revise BTP 7-19 again, without addressing these additional new sources of CCF, at least to the same extent as software defects, fails to address the fundamental intent of SECY 93-087, which is to address new sources of CCF in digital systems.

The BTP emphasis on software defects is more than just technically unjustified and noncompliant to SECY 93-087. Most importantly, it is likely to lead designers and NRC reviewers to focus on software defects at the expense of thoroughly evaluating the potential for other CCF sources that are much more likely.

This BTP title should be changed to "Guidance for evaluation of CCFs in DI&C Systems", and the BTP should be expanded to provide guidance for addressing CCFs caused by system/hardware design defects, and random hardware failures.

<u>NRC Staff Response</u>

The NRC staff agrees with the comment that hardware design defects and random failures, as well as failures occurring in shared resources, may also result in CCFs, but does not agree with the proposed change identified by the comment. Specifically, the staff declines to expand the BTP as suggested by the comment because other staff guidance addresses the topics the comment identifies as missing from the BTP. In the BTP, the staff has elected to focus on aspects of addressing CCF that have not been addressed through other NRC staff guidance, industry standards, or industry guidance. For BTP 7-19, the staff identified that guidance needed to be clarified regarding how reviewers should evaluate applications that address possible beyond design basis CCFs that result from latent design defects. In Section A. "Background" of the BTP, the staff described latent design defects, including the concept that latent design defects may exist in both hardware and software. Regarding CCFs that can result from single failures being propagated to adversely affect multiple design functions in a cascaded manner, the staff identified that such failures are "design basis events," which are evaluated as part of the single-failure analysis requirements covered within applicable IEEE standards and are not covered by the BTP. Pointers to applicable guidance for cascaded failures were placed into the Background and Scope subsections of Section A. In addition, the title of this BTP was modified to better reflect its purpose and scope, although the staff did not adopt the title suggested in the comment.

Comment No. 2-2

There is no licensing basis or regulatory guidance precedence, including consideration of SECY 93-087, for the acceptance criteria distinction in Section 3.3, for anticipated operational occurrences (AOO) and postulated accidents (PA).

As stated previously in this BTP, the SRM to SECY 93-087, states that a CCF [due to a design defect] is a BDBE, therefore an AOO or PA with concurrent CCF are both BDBEs. When considering the potential frequency of these events, the difference in safety significance is negligible. In addition, to distinguish compliance to offsite dose limits vs. 10% of offsite dose limits is not consistent with the use of best-estimate methods (permitted by SECY-93-087), which typically employ assessments of core coolability, primary coolant and containment boundary integrity. Extending these assessments to accurately determine offsite dose requires much more burdensome modeling and analysis that is not consistent with evaluation of BDBEs or best-estimate methods.

The same acceptance criteria, as stated for a PA, should apply to both PAs and AOOs. If the Staff believes there is a licensing basis for different acceptance criteria, or justification for the analysis burden associated with precise offsite dose determination, then that basis/justification should be explained.

NRC Staff Response

The NRC staff disagrees with the comment's assertion that the same acceptance criteria stated for a PA should also apply to AOOs. The staff may reconsider this assertion in future revisions to the BTP upon further review and public discussion. The staff notes that previous versions of this BTP dating back to 1997 have included this acceptance criterion for a PA, without feedback from stakeholders regarding any associated analysis burden. The staff recognizes that a CCF concurrent with an AOO is a beyond design basis event (BDBE). The difference in acceptance criteria, however, between AOOs and PAs reflects generic qualitative risk considerations: an AOO is expected to occur during the lifetime of a plant whereas a PA is not expected to occur. The AOO acceptance criterion is generally consistent with Chapter 15, "Transient and Accident Analysis," of NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition," in which AOOs are expected to have no-to-minimal dose consequences. The guidance of this BTP maintains this distinction with regard to the relaxed criteria that permits the use of best-estimate analysis methodology for beyond-design-basis CCF events. The staff has determined there is not a sufficient technical or regulatory basis for making a change of this type to the BTP at this time. Therefore, the NRC staff made no changes to the BTP as a result of this comment.

Comment No. 2-3

The acceptance criteria in Section 5 needs to distinguish spurious operations caused by a single random hardware failure and spurious operations caused by a single design defect.

A single random hardware failure is a DBE expected during the life of the plant; therefore, the resulting spurious operations always require conservative DBE analysis methods and the plant level results must always be bounded by current AOOs, or new AOOs must be added to the TAA. On the other hand, a design defect is not expected to be triggered during the life of the plant; therefore, the resulting spurious operations can be analyzed using best-estimate BDBE analysis methods and the plant level results can meet the same acceptance criteria as defined for a PA in Position 3.

NRC Staff Response

The NRC staff agrees with the comment that spurious operations can be caused by either single random hardware failures (which are expected during the life of the plant), or by design defects. The staff revised BTP 7-19 to clarify guidance to the staff for reviewing evaluations of spurious operation resulting from CCFs due to design defects, including guidance for reviewing an applicant’s use of best-estimate methods. That guidance has been integrated into Section B.3 to clarify how the guidance should be considered in the overall review for CCF. Further, Section A.3 “Scope” of the BTP has been revised to identify that staff review criteria for single random failures and shared resource cascading failures not due to latent design defects in digital I&C SSCs are not covered in this BTP. Guidance for addressing single failures in systems credited to perform safety functions is provided in Regulatory Guide 1.53, “Application of the Single Failure Criterion to Safety Systems,” which points to applicable criteria in the IEEE Standards. Also, SRP Section 7.7, “Control Systems,” provides guidance for the analysis of postulated failures in NSR systems. In addition, a footnote has been added in Section B.3 to highlight the fact that spurious operation can occur from a single failure. This footnote states: “Spurious operations addressed “within the design basis” include spurious operations that occur as a result of single failures (including cascading effects) or single malfunctions. Consistent with regulatory requirements such as those of GDC 25 or incorporated by reference in 10 CFR 50.55a(h) (IEEE Std 279-1971 or IEEE Std 603-1991), spurious operations as a result of single failures and single malfunctions are expected during the lifetime of the plant and are addressed as part of the design basis.”

Comment No. 2-4

Section 5.2.b.3.ii states that “The quality development process of an A1 system or components may be credited to reduce the likelihood of CCF hazards that could lead to spurious operation of a safety function.” This is correct for a CCF due to a design defect. This is not correct for a CCF due to failure of a shared hardware resource, which is a random DBE event that must be expected during the life of the plant and therefore analyzed conservatively.

NRC Staff Response

The NRC staff agrees with the comment that the quality development process of a highly safety significant (formerly identified as A1) system or components may be credited to reduce the likelihood of CCFs due to design defects that could lead to spurious operation of a safety function. The staff also agrees with the comment that this crediting would not be appropriate for a CCF due to a single random failure of a shared hardware resource. Such random failures of shared resources must be analyzed as DBE events through application of the single failure criterion, and are analyzed conservatively. Section A.3 “Scope” of the BTP has been revised to clarify that staff review criteria for single random failures and shared resource cascaded failures in digital I&C SSCs are not covered in this BTP. The staff also revised Section B.3 of BTP 7-19 to provide clear guidance for evaluating spurious operation resulting from CCFs due to design defects, including guidance for evaluating an applicant’s use of best-estimate methods. Finally, a footnote has been added in Section A to clarify what guidance may be used for reviewing licensee analyses of spurious operation resulting from single failures. This footnote states: “Spurious operations addressed “within the design basis” include spurious operations that occur as a result of single failures (including cascading effects) or single malfunctions. Consistent with regulatory requirements such as those of GDC 25 or incorporated by reference in 10 CFR 50.55a(h) (IEEE Std 279-1971 or IEEE Std 603-1991), spurious operations as a result of single failures and single malfunctions are expected during the lifetime of the plant and are addressed as part of the design basis.”

Comment No. 2-5

Section 5.2.b.3.ii states that “As such, the application should demonstrate that the initiating event created by potential spurious operation of a single safety function (e.g., spurious operation of both emergency core cooling system trains)...” There is no technical basis for limiting the initiating event to a single safety function.

A single design defect in a software function block would affect all safety functions that utilize that software function block in one or multiple processors. Similarly, a single random failure in a hardware memory block would affect all safety functions in the same processor that utilize that hardware memory block. Without adequate defensive measures, there are also other random hardware failure vulnerabilities that could adversely affect all safety functions controlled by the same or multiple processors.

NRC Staff Response

The NRC staff agrees with this comment. The BTP guidance cited has been relocated to Section 6.1 and the text was revised to describe a software function block. This section provides clarification on the possible effects of failures that can occur when a software function block is used by multiple design functions that use the same software (within the logic or divisions). Specifically, the BTP was revised to explain that when a block is used by multiple design functions using the same software (within the logic or divisions), a failure within the block can result in a CCF of all design functions that use that block.

Comment No. 2-6

Section 5.2.c.1 states that the likelihood of a CCF that leads to spurious operation can be reduced to a “sufficiently low” level using qualitative measures. This is technically correct for a CCF due to a design defect; but is incorrect for a CCF due to a random hardware failure, because random hardware failures must be assumed to occur during the life of the plant. Therefore, there are no qualitative measures that can reduce the likelihood of a CCF due to a random hardware failure to "sufficient low". To preclude the need for further consideration, deterministic defensive measures are required to ensure a random hardware failure does not result in a CCF.

NRC Staff Response

The NRC staff agrees with the comment that the likelihood of a CCF due to a latent design defect that leads to spurious operation can be reduced to a "sufficiently low" level using qualitative measures; however, single random failures are outside the scope of the BTP as clarified in a new footnote in Section A.3 of the BTP. No change was made as a result of this comment."

Comment No. 2-7

Section B.3.1.1.b refers to "adequate diversity," but does not define "adequate". Add: "Adequate diversity" is diversity sufficient to preclude concurrent triggers of a design defect, even if a common design defect coexists in the diverse portions of the system. To credit non-concurrent triggers, the failure must be self-announcing and quickly correctable prior to an expected need for the system. The time for an expected need can credit technical specification limiting conditions of operation. For example, a triggered defect in one safety division may require plant shutdown with a relatively short completion time. When the plant is shutdown, the system may no longer be needed."

NRC Staff Response

The NRC staff does not agree that "adequate diversity" needs to be defined. Rather than relying on a definition, the staff structured the BTP to define the acceptance criteria for the staff to use for evaluating whether the applicant has reasonably demonstrated that a proposed plant design for digital SSCs has defense-in-depth, which may be achieved by including the use of design diversity. This approach provides more flexibility for staff reviewers as well as designers to account for the nuances of their individual systems. The BTP was revised to provide the acceptance criteria in section B.3.1.1. The section states that if diversity is used, a latent design defect in one portion of a system or component would not result in a failure in the diverse portion of the system or component. In particular, the BTP directs the reviewer to determine whether the application includes an analysis comparable to the guidance of NUREG/CR-6303 and NUREG/CR-7007 to demonstrate that the diversity attributes between different divisions of the digital protection system are adequate to eliminate a CCF such that further consideration is unnecessary.

Comment No. 2-8

The Rev. 7 discussion of partial CCF should not have been removed. Partial CCFs are a valid concern, because digital systems can have a defect that is triggered in specific distributed component control processors, but not triggered in initiation processors. If the DAS monitors selected ESF components to determine when its actuation is needed (i.e., when there is an actual CCF), then a partial CCF could prevent actuation of the DAS (or a specific DAS function) when it is needed.

NRC Staff Response

The NRC staff understands the comment to request the staff to add back the discussion on partial actuation that was in Section 1.8 of BTP 7-19, Revision 7. The staff generally agrees with the comment and has modified BTP 7-19, Revision 8, to add back the discussion on partial actuation that previously existed in Section 1.8 of BTP 7-19, Revision 7. However, due to other edits, the description of partial CCF was placed into Section B.3 of the document. Specifically, the following guidance was added into Section 3.0: “For example, a partial actuation of an emergency core cooling system (i.e., spurious operation of a single division) with false indication of a successful actuation may take an operator longer to evaluate and correct than would a total failure to send any actuation signal. Therefore, the reviewer should consider both the possibility of partial actuation and total failure to actuate, together with false indications, stemming from a CCF.”

Comment No. 2-9

For the description of safety significance categories B1 and B2, delete the second paragraph. There is no way of knowing if a failure does or does not have consequences, or can or cannot be mitigated, until the assessment is done. If the failure challenges a critical safety function, as identified in the paragraph above, an assessment is needed; if there is no challenge to critical safety functions an assessment is not needed.

NRC Staff Response

The NRC staff agrees with the comment but has chosen not to address it in the manner suggested. Due to other edits made in the same section, the table (Table 2-1) that appeared in Section B.2 of the draft Revision 8 of BTP 7-19 was removed. Instead, the proposed guidance regarding a graded approach was revised to use a safety significance determination. The revised staff guidance describes how a staff reviewer would evaluate alternate methods that applicants may propose for performing defense-in-depth and diversity analyses, based on the results of determining the safety significance of the function performed, which may include the results of a failure consequence analysis. The new section provides acceptance criteria for a staff reviewer to use when evaluating applications describing the relative safety-significance of the functions performed by an SSC. This section also describes how to evaluate an application that does not include a D3 assessment for the lowest safety-significant SSC.

Comment No. 2-10

For the description of safety significance category A2, delete the second paragraph. Maintaining safe shutdown is as risk significant as achieving safe shutdown. Therefore, the equipment directly credited to maintain safe shutdown (e.g., residual heat removal pumps) is A1.

NRC Staff Response

The NRC staff agrees with this comment. The staff modified the acceptance criteria in Section B.2 to identify equipment relied upon for maintaining the plant in a safe-shutdown condition as being within the highest safety significance category. However, due to edits made to address other comments within the same section, the table (Table 2-1) that appeared in Section B.2 of the draft Revision 8 of BTP 7-19 was removed. Instead, the proposed guidance regarding a graded approach was revised to use a safety significance determination. The revised staff guidance describes how a staff reviewer would evaluate alternate methods that may be proposed by applicants for performing defense-in-depth and diversity analyses, based on safety significance of the function performed, which may include the results of a failure consequence analysis. The new section provides a description of how a staff reviewer would evaluate applications describing the relative safety significance of the functions performed by an SSC.

Comment No. 2-11

Several sections identify "defensive measures" as a means to preclude further consideration of a CCF due to a design defect. Sufficient diversity and testability are defensive measures. I know of no other defensive measures that can eliminate further consideration of a CCF due to a design defect. Other defensive measures are applicable to preventing CCF due to random hardware failures in shared resources. For example, compliance to the communication independence guidance in ISG-04 is a defensive measure against a CCF of multiple processors due to a data storm.
In the context of eliminating CCF due to a design defect other defensive measures should be deleted; alternately, the Staff should provide an example of another defensive measure.

NRC Staff Response

The NRC staff disagrees with the proposed change. The NRC staff revised BTP 7-19, Revision 8, to provide technical reviewers with additional flexibility for evaluating applications that address CCF vulnerabilities in digital I&C systems using NRC-approved alternative measures, which would include concepts such as defensive measures, provided a sufficient technical basis exists. While the NRC staff agrees that sufficient diversity and testability are the only approved design attributes at this time, the NRC staff is allowing for the possibility of alternative methods, including new and innovative design techniques and design features such as defensive measures. The staff modified BTP 7-19, Revision 8, to allow for the use of NRC-approved alternative methods such as defensive measures. The BTP also acknowledges that reviewers can consider the use of alternative methods not previously approved on a case-by-case basis, if sufficient technical justification is included in the application. If no defensive measures are approved as design attributes that serve to eliminate CCF from further consideration, the staff would consider whether further revision of this document is needed. In future revisions to the BTP, the staff will consider providing additional guidance to reviewers based on any experience gained with additional alternative methods reviewed under Revision 8.

Comment No. 2-12

Section 3.2.c requires "sufficiently independent" instrumentation. Delete "sufficiently independent". There is no requirement for independent instrumentation. The only requirement is that the instrumentation credited for CCF mitigation not be subject to the same defect that led to the CCF.

NRC Staff Response

The NRC staff agrees with this comment. The staff revised BTP 7-19, Revision 8, where appropriate, to eliminate the term "sufficiently independent" and instead use the term "independence" in a manner consistent with its context in any applicable regulatory requirements or Commission policy. In addition, the BTP states that alternate means of accomplishing the same design functions should not be susceptible to the same CCF vulnerabilities. The staff also revised the BTP to provide clear guidance to reviewers for evaluating proposed designs for meeting Position 3 versus Position 4 of SRM-SECY 93-087.

Comment No. 2-13

Section 3.2.1 has distinct guidance for crediting existing systems. The same guidance applies whether a system credited for CCF mitigation is new or existing. This distinction is technically unnecessary and adds unnecessary complexity to the document.

NRC Staff Response

The NRC staff agrees that most of the guidance in the BTP for a diverse means to mitigate CCF is similar for both existing and new systems. For example, the acceptance criteria for crediting both existing and new diverse means are very similar, and even overlapping in certain areas. In the NRC staff's experience, however, the reviews are sufficiently different that reviewers will benefit from separate guidance for consideration of the two ways to provide a diverse means. The BTP was clarified to better reflect the differences and similarities between reviews of the two different types of systems. The BTP focuses on the following two differences in the NRC review applied to existing or new diverse systems.

If the LAR credits an existing system, the application will necessarily need to develop a new basis to demonstrate that the existing system is not subject to the same CCF as the proposed digital I&C system. The reviewer will need to consider whether the LAR adequately accounted for all the existing system's design attributes and requirements and potential interconnections. In addition, the reviewer should consider whether the LAR accounts for the established licensing basis of the existing system, e.g., the system's other credited functions. In contrast, if the LAR credits a new diverse system, the new system design documentation will include diversity and will document system features, such as potential interconnections, that may affect diversity.

In addition, the NRC staff added guidance to consider the prioritization scheme when actuating shared components. For crediting existing systems, the applicant needs to consider whether the prioritization scheme is either maintained or being modified. For new systems, the applicant would define the new prioritization scheme to be implemented to ensure safety and protection system functions have the highest priority when components are shared with control systems.

Comment No. 2-14

This document incorrectly uses the terms "failure" and "CCF". For example, Section A states "A CCF of a DI&C system or component can also initiate the operation of a safety-related function...", but erroneously initiating the operation of a single safety function that effects only a single safety component is not a CCF. Similarly, Section B 1.1 states "If the D3 assessment shows a postulated CCF could disable a safety function ...", but a safety function must be disabled in multiple safety divisions for it to be a CCF.

In this BTP, the distinction between "failure" and "CCF" should be clearly defined. For example: A design defect or random hardware failure can cause failure-to-actuate and/or erroneous operation of a single function or plant component, or failure-to-actuate and/or erroneous operation of multiple functions or multiple plant components. When either failure source affects multiple functions or multiple plant components (in a single or multiple divisions), the failure is a CCF. When either failure source affects only one function and/or only one plant component, the failure is not a CCF.

NRC Staff Response

The NRC staff agrees with the comment that the draft BTP was not as consistent as it could have been regarding the application of the term “CCF.” The staff modified the Background section and several other sections within BTP 7-19, Revision 8 to ensure proper consistency in the use of the terms “failure” and “CCF.” In a similar manner, as described in the responses to Comments 2-3 and 2-4 above, the staff also modified the BTP to ensure consistency in the distinction between CCFs due to single random hardware failures and CCFs due to latent design defects.

Comment No. 2-15

There is no value in including the word "hazard" throughout this document, because all shared design and shared hardware resources must be evaluated to identify CCFs. If the CCF susceptibility evaluation demonstrates that a CCF from a shared resource is not prevented, an additional plant level evaluation is needed to determine if there is not a new unanalyzed plant condition, or if the new plant condition is effectively mitigated. If the staff believes there are potential sources of CCF that do not require evaluation, an example should be provided.

NRC Staff Response

The NRC staff agrees with this comment. The staff modified BTP 7-19, Revision 8, to eliminate the use of the term “hazard.”

Comment No. 2-16

The addition of “errors in the higher-level requirements” on page 10 requires clarification. Add: SECY 93-087 was written to address new sources of CCF that apply to digital systems that did not apply to analog systems. Therefore, this BTP excludes consideration of errors in functional requirements for safety systems, which are independent of technology implementation. In combination, compliance to the functional diversity requirements of GDC 22, modeling of safety system functions in the transient and accident analysis, and quality assurance programs, assure that errors in functional requirements require no further consideration.

NRC Staff Response

The NRC staff agrees that the phrase “errors in the higher-level requirements” was unclear. The staff revised BTP 7-19, Revision 8 to eliminate reference to “errors in higher-level” system requirements. The BTP refers to the use of a robust (high-quality) development process and system analysis to address potential design errors in the system or component requirements or specifications, so the evaluation of such higher-level requirements considerations is outside the scope of this BTP.

Comment No. 2-17

Although the staff does not review modifications performed under the 10 CFR 50.59, “Changes, Tests and Experiments,” change process, as stated in Section A.3, this BTP should state that licensees should consider the technical guidance in this BTP when making those changes.

NRC Staff Response

The NRC staff disagrees with this comment. The staff revised BTP 7-19, Revision 8, Section A.3, to clearly state that the BTP is intended for staff reviews of I&C safety systems proposed (1) in requests for license amendments as modifications to licensed nuclear power plants, and (2) in applications for CPs, OLs, COLs, DCs, SDAs, and MLs. The guidance for staff reviewers stated in the BTP is irrelevant to implementation by licensees of the requirements of 10 CFR 50.59. No changes were made to the BTP as a result of this comment.

Letter 3—Comments from SunPort

The review guidance for the treatment of beyond design basis condition (i.e., CCF causing spurious operation) in NSR equipment lacks a clear, integrated, and coherent regulatory basis. Draft Revision 8 of Branch Technical Position 7-19 adds to the confusion. It does not integrate the other review guidance in SRP Section 7.7 or DI&C-ISG-04, Revision 1, regarding spurious actuations caused by safety-related and NSR digital I&C equipment. It also does not clearly establish the regulatory basis for the various technical positions, especially regarding NSR digital I&C systems not directly connected to safety-related components. A full set of comments is provided as an attachment.

Note: The NRC staff has determined that Letter 3 was submitted in error. The submittal has no attachments. The above comment from Letter 3 is a duplicate of comment 4-1. However, Letter 4 contains the attachment mentioned in Letter 3. The NRC staff addressed the comments in Letter 3 in response to Letter 4.

Letter 4—Comments from SunPort

Note: The attachment to Letter 4 provided suggested edits to draft BTP 7-19, Revision 8, for the NRC staff's consideration with each of the comments below. The NRC staff will address the edits as applicable to each comment below.

Comment No. 4-1

The review guidance for the treatment of beyond design basis condition (i.e., CCF causing spurious operation) in NSR equipment lacks a clear, integrated, and coherent regulatory basis. Draft Revision 8 of Branch Technical Position 7-19 adds to the confusion. It does not integrate the other review guidance in SRP Section 7.7 or DI&C-ISG-04, Revision 1, regarding spurious actuations caused by safety-related and NSR digital I&C equipment. It also does not clearly establish the regulatory basis for the various technical positions, especially regarding NSR digital I&C systems not directly connected to safety-related components. A full set of comments is provided as an attachment.

NRC Staff Response

The NRC staff agrees with the comment that the regulatory basis was not clearly stated. SRP Section 7.7 and ISG-04 were added as references to the BTP. An applicant can use these documents if the applicant chooses to employ the conservative methods that they describe. The draft BTP revision 8 clarifies the regulatory basis and analytical methods under the D3 assessment the staff finds adequate to address spurious operations as a result of CCF originating from latent design defects. This includes specific guidance for analytical methods appropriate for SSCs of varying safety significance, as described in Section 2 of the BTP. The staff also added clarifying guidance on the technical and regulatory basis for reviewing NSR digital I&C systems. The BTP also provides guidance for addressing CCF of different SSCs with varying safety significance that may share resources or are integrating in their design functions. No changes other than those described above in this response were made as a result of this comment.

Comment No. 4-2

Background

Standard Review Plan (SRP) Section 7.7 has some limited guidance for the treatment of control system failures causing spurious operations. The guidance is confusing because it introduces the ideas of software design errors and random hardware failures but also says that the evaluation of multiple independent failures is not intended.

DI&C-ISG-04, Revision 1, addresses malfunctions and spurious actuations in non-safety related (NSR) control systems. The guidance is incomplete in that it only identifies failure conditions that should be addressed but does not address the evaluation methodologies or acceptance criteria.

SRM-SECY-93-087 is the current basis for the NRC position on digital CCFs. Point 1 – 3 do not explicitly address treatment of new postulated beyond design basis conditions caused by CCFs resulting in multiple spurious operations in safety-related or NSR equipment.

Draft Revision 8 of Branch Technical Position (BTP) 7-19 is proposing changes to the guidance regarding the treatment of malfunctions and spurious actuations in NSR control systems. It makes the broad statements that IEEE Std 603-1991, Clauses 4.8 and 5.6.3, provide the basis for requiring licensees to address the potential for spurious operation of safety-related components and components that are NSR. This position requires a new understanding of the standard and not consistent with other governing regulatory criteria.

NRC Staff Response

The NRC staff understands the comment is questioning the regulatory basis for considering evaluating spurious operation in NSR SSCs. In addition, the comment indicates that the guidance in SRP Section 7.7 is confusing and the guidance in DI&C-ISG-04 is incomplete. The NRC disagrees with these comments. The NRC staff has determined that spurious operation is a potential outcome of CCF originating from latent design defects. Consistent with the Commission's direction in SRM-SECY 93-087, CCF resulting from latent design defects and any resulting effects, including spurious operation, are beyond design basis events. Beyond design basis events necessitate specific design or analytical solutions. This BTP revision clarifies its regulatory basis and the analytical methods under the D3 assessment that the staff finds acceptable to address spurious operations as a result of CCF originating from latent design defects. To the extent that the commenter has identified issues in the SRP 7.7 and ISG-04, such issues do not affect the use of BTP 7-19. Regarding the comment about SRP Section 7.7 and DI&C-ISG-04, these documents are out of the scope of this BTP.

Comment No. 4-3

Problems with Draft Revision 8 of Branch Technical Position 7-19

The review guidance for the treatment of beyond design basis condition (i.e., CCF causing spurious operation) in NSR equipment lacks a clear, integrated, and coherent regulatory basis. Draft Revision 8 of Branch Technical Position 7-19 adds to the confusion. It does not integrate the other review guidance in SRP Section 7.7 or DI&C-ISG-04, Revision 1, regarding spurious actuations caused by safety-related and NSR digital I&C equipment. It also does not clearly establish the regulatory basis for the various technical positions, especially regarding NSR digital I&C systems not directly connected to safety-related components.

IEEE Std 603-1991, Clauses 4.8 and 5.6.3 are relevant for the case where NSR systems can directly actuate safety-related systems or components. On the other hand, it requires new and different interpretations of the terminology used is these requirements to extend applicability to NSR systems or components that are not directly connected to safety-related equipment. It is not clear what the regulatory basis for the treatment of spurious actuation hazards would be for plants with IEEE Std 279 as their licensing basis.

It is not consistent to use Clause 4.8 to conclude a new postulated beyond design basis condition (CCF causing spurious operation in NSR equipment that has no direct connection to safety-related equipment) as part of defined safety function (i.e., design basis condition) or that it causes degradation of a safety-related system.

It is also not appropriate to use Clause 5.6.3 to conclude a new postulated beyond design basis condition (CCF causing spurious operation in NSR equipment that has no direct connection to safety-related equipment). Clause 5.6.3.1, Interconnected Equipment, is not applicable to NSR equipment with no direct connection to safety-related equipment. Clause 5.6.3.2, Equipment in Proximity, requires physical separation, which is not relevant to the postulated CCF scenarios for NSR equipment. Clause 5.6.3.3, Effects of a Single Random Failure, addresses the case where a single random failure in a nonsafety system can (1) result in a design basis event, and (2) also prevent proper action of a portion of the safety system designed to protect against that event, the remaining portions of the safety system shall be capable of providing the safety function even when degraded by any separate single failure. This clause would require assessment of random hardware failures associated with shared hardware resources in NSR distributed control systems; however, it does not address beyond design basis conditions caused by postulated software CCFs in NSR equipment.

SRM-SECY-93-087 is cited as the basis for the NRC position on digital CCFs. Point 1 in the SRM addresses the need to assess potential CCF vulnerabilities. Point 2 addresses how diversity can be used to address the CCF vulnerabilities for each accident event analyzed in the FSAR. Point 3 addresses how the CCF vulnerabilities can be mitigated by diverse actuations. Points 1 – 3 do not explicitly address treatment of new postulated beyond design basis conditions caused by CCFs resulting in multiple spurious operations in safety-related or NSR equipment. Clearly the existence of NSR distributed control systems and digital human-machine interfaces were contemplated at the time SECY-93-087 was written (as discussed in SECY-91-292) yet these digital systems were not included in the Commission directions to the staff.

The review guidance in SRP Section 7.7 is based on IEEE Std 603-1991 Clause 5.6.3. The concern with random hardware failures associated with shared hardware resources in NSR *distributed control systems fits the context of IEEE Std 603-1991 Clause 5.6.3.3; however, the treatment of other postulated multiple spurious actuations is not consistent with the governing regulatory criteria. SRP Section 7.7 also references SRM-SECY-93-087 to the extent that control system functions are credited as diverse means for performing safety functions to satisfy Point 3 in SRM-SECY-93-087; however, it is not used to address beyond design basis conditions caused by postulated software CCFs in NSR equipment.*

NRC Staff Response

The NRC staff understands the comment is questioning the regulatory basis for considering evaluating spurious operation caused by CCFs in NSR SSCs. The NRC disagrees with the comment. The NRC staff has determined that spurious operation is a potential outcome of CCF originating from latent design defects. Consistent with the Commission's direction in the SRM-SECY 93-087, CCF resulting from latent design defects and any resulting spurious operation are beyond design basis events and necessitate specific design and/or analytical solutions in an application that employs digital technology. CCFs resulting from latent design defects are the focus of this BTP, whose regulatory basis is established by SRM-SECY-93-087. The BTP also provides guidance for addressing CCF of different SSCs with varying safety significance that may share resources or are integrated in their design functions. This BTP revision clarifies the regulatory basis for addressing spurious operations as a result of CCF originating from latent design defects and the analytical methods for the D3 assessment the staff evaluates in that regard. This BTP also provides reference to SRP Section 7.7 and DI&C-ISG-04, as necessary.

Comment No. 4-4

A Deeper Look at IEEE Std 603

The IEEE Std 603 issues are summarized in Table 1. The items in ***bold italics*** *are the issues that are introduced but not well-defined in BTP 7-19 draft revision 8.*

Table 1 – Summary of Issues

Safety-Related Controls with Direct Connection to Safety Components		Non-Safety Related Controls with Direct Connection to Safety Components		Non-Safety Related Controls with No Direct Connection to Safety Components	
Design Basis	Beyond Design Basis	Design Basis	Beyond Design Basis	Design Basis	Beyond Design Basis
Single failure criterion and consequential failures caused by design basis event (Clause 5.1) Qualification for environment and external events to avoid hardware CCF (Clauses 4.h and 5.2)	Software CCF to prevent actuation (Clause 4.12 has been cited for some license amendment requests) ***Software CCF from control room HMI causes spurious actuation (only new plant precedents)***	Credible failures in and consequential actions by other systems, as documented in Clause 4.h of the design basis (qualification), shall not prevent the safety systems from meeting its requirements. Requirements for isolation, physical separation and consideration of single random failures are specified. (Clause 5.6.3)	***Software CCF in control systems and control room HMI causes spurious actuation of safety- related components***	No requirements in IEEE Std 603	***Software CCF in control systems and control room HMI causes spurious actuation of non safety-related components that represent new transients not evaluated in Chapter 15***

Note: Protection system safety functions are derived from analysis of specific postulated initiating events in FSAR Chapter 15, which have been standardized in SRP Chapter 15. (Clauses 4.1 and 4.2)	Note: CCF from ESFAS not generally considered as source of spurious actuation in approved precedents	Note: It is often considered that the design basis events evaluated in Chapter 15 are related to a failure assessment of the non-safety related systems, but they are not. There are some events that are specified for evaluation in SRP Chapter 15 that would only occur with multiple non-mechanistic failures (e.g., loss of all feedwater, loss of feedwater enthalpy, etc.).

NRC Staff Response

The NRC staff understands the comment to provide recommendations on how SSCs of different safety significance should be treated in the BTP based upon the comment's focus on IEEE Std. 603-1991. The NRC agrees in part with these comments. This revision of the BTP clarifies the differences in regulatory treatment between failures that are addressed within the design basis (e.g., single failures and single failures with cascading effects) and CCFs due to latent design defects (the subject of this BTP), which are beyond design basis. The BTP also provides guidance for addressing CCF of different SSCs with varying safety significance that may share resources or are integrated in their design functions. Consistent with the Commission's direction in SRM-SECY 93-087, CCF resulting from latent design defects and their potential outcomes (i.e. loss of function or spurious operation) are considered beyond design basis. This BTP revision clarifies the regulatory basis for addressing spurious operations as a result of CCF originating from latent design defects and the analytical methods for the D3 assessment the staff evaluates in that regard. No further changes were made as a result of this comment.

Comment Nos. 4-5(a) and 7-1

Conflicts with Other NRC Review Guidance

(Comment No. 4-5(a)): *Observation: The guidance in SRP 7.7 is confusing because it suggests that postulated NSR failures that can cause spurious actuations must meet the acceptance criteria for anticipated operational occurrences (i.e., treated as design basis events). However, the actual practice for new plants reviews and the direction taken in Draft Revision 8 of BTP 7-19 is that certain postulated failures in NSR systems that affect spurious actuation of multiple components can be treated as beyond design basis events with other acceptance criteria.*

(Comment 7-1) *The words "failure of any control system component" is commonly understood to refer to a random hardware component failure, not a design defect. Since random hardware failures are expected to occur during the life of the plant, the SRP is correct in that the plant level results of a random hardware failure (i.e., any component) should be treated as an anticipated operational occurrence (AOO), which is a design basis event (DBE). On the other hand, spurious operations due to a design defect are not expected to occur during the life of the plant because (1) the rigorous design processes applied to the control systems covered by SRP Section 7.7 make design defects unlikely, and (2) while there is no claim for defect free designs, the unusual conditions needed to trigger a defect are not expected to occur during the life of the plant. Therefore, for new plants, erroneous operations due to a design defect have been treated as beyond design basis events (BDBE) with relaxed analysis methods (e.g., best-estimate) and relaxed plant level acceptance criteria (e.g., as required for postulated accidents, not AOOs). BTP 7-19 should clearly make these distinctions for NSR control systems as well as SR systems within the same safety division.*

NRC Staff Response to Comment 4-5 and Comment 7-1

The NRC staff understands that both comments are concerned with SRP Section 7.7 as it pertains to failures in NSR systems that can lead to outcomes such as spurious operation. However, SRP Section 7.7 is out of scope for this BTP update, so the staff is not addressing the comment related to SRP Section 7.7. Revision 8 to BTP 7-19 clarifies guidance on spurious operation caused by CCF. Also, this revision clarifies the BTP's guidance for reviewing a D3 assessment to SSCs of varying safety significance as described in Section 2 and 3 of the BTP.

Further, consistent with the Commission's direction in SRM-SECY 93-087, CCF resulting from latent design defects and their potential outcomes (i.e., loss of function or spurious operation) are considered beyond design basis. The staff has revised the BTP to clarify that all CCFs resulting from latent design defects, including those that result in spurious operation, are beyond design basis events.

With regard to comment 7-1, the revised guidance provides staff with ways to review applications that use different methods to address spurious operations. The revised guidance also clarifies the scope of the BTP to cover CCF that result from latent design defects in hardware, software, and software-based logic. This revision clarifies that latent design defects that result in CCF, leading to a loss of function or spurious operation, are beyond design basis events and is the subject of this BTP. For SSCs of varying safety significance and different safety classifications, the BTP was revised to clarify acceptable analytical approaches under a D3 assessment. This revision also makes it clear that an applicant can use conservative design analysis or realistic assumptions (e.g., realistic acceptance criteria) as part of the D3 assessment, regardless of the safety classification of the SSC in question. No changes were made as a result of these comments.

Comment Nos. 4-5(b) and 7-2

Conflicts with Other NRC Review Guidance

(Comment 4-5(b)) *Observation: The guidance in SRP 7.7 is also confusing regarding the statement "evaluation of multiple independent failures is not intended," since it is not clear whether meeting the physical separation and electrical isolation (i.e., independence) required by IEEE Std 603-1991 Clause 5.6.3 is sufficient (i.e., independence for a direct connection between a safety-related and NSR system meeting the requirements of IEEE Std 384 is sufficient. That same statement has also been used to require additional features within an NSR system design to provide some other type of 'independence' (e.g., controller segmentation) that has no established regulatory definition.*

(Comment 7-2) *BTP 7-19 should clarify the distinction between inter-division independence and intra-division independence. In accordance with IEEE-603, RG 1.75 and IEEE-384, inter-division independence must accommodate single random hardware failures, as well as fire (within enclosures), flood and electrical faults. Traditionally, when considering intra-division independence, only random hardware failures have been evaluated. The difference is based on the expected likelihood of these events, as discussed above. BTP 7-19 should also clarify that common intra-division design features, such as segmentation, cannot prevent erroneous signals that may be generated by a random hardware failure or design defect in one segment from propagating to other segments; other defensive measures are also required. Equally important is that without adequate defensive measures, a random hardware failure or design defect in a shared resource, such as a communication network or visual display unit, can adversely affect multiple segments.*

NRC Staff Response to Comment 4-5(b) and Comment 7-2

The NRC staff understands the comments to state that SRP Section 7.7 has some confusing language with regard to multiple independent failures. The staff also understands comment 7-2 as suggesting the BTP should be updated to clarify independence and single failure considerations in the BTP. SRP Section 7.7 is out of scope of this BTP revision. With regard to the concepts of independence and single failure, these are design basis considerations covered under separate design basis requirements. These requirements are not the subject of this BTP, and other SRP sections provide guidance for reviewing a design with respect to these requirements. Although no change was made to the document as a result of these comments, the NRC staff clarified in the BTP the difference in regulatory treatment between failures and effects due to random hardware failures and failures due to latent design defects.

Comment Nos. 4-6 and 7-3

Conflicts with Other NRC Review Guidance

(Comment 4-6)
DI&C-ISG-04, Revision 1, provides review guidance for assessing the effects of spurious actuations from control system failures in Section 3.1.5 (bulleted items) that should be clarified and considered in Draft Revision 8 of BTP 7-19:

- *Safety and control processors should be configured and functionally distributed so that a single processor malfunction or software error will not result in spurious actuations that are not enveloped in the plant design bases, accident analyses, ATWS provisions, or other provisions for abnormal conditions. This includes spurious actuation of more than one plant device or system as a result of processor malfunction or software error. The possibility and consequences of malfunction of multiple processors as a result of common software error must be addressed.*

Observation: This guidance in DI&C-ISG-04 is confusing because it suggests that postulated safety-related and NSR failures that can cause spurious actuations must meet the acceptance criteria for anticipated operational occurrences (i.e., treated as design basis events). However, the actual practice for new plants reviews and the direction taken in Draft Revision 8 of BTP 7-19 is that certain postulated failures in NSR systems that affect spurious actuation of multiple components caused by common software errors can be treated as beyond design basis events with other acceptance criteria.

- *No single control action (for example, mouse click or screen touch) should generate commands to plant equipment. Two positive operator actions should be required to generate a command. For example: When the operator requests any safety function or other important function, the system should respond “do you want to proceed?” The operator should then be required to respond “Yes” or “No” to cause the system to execute the function. Other question-and-confirm strategies may be used in place of the one described in the example. The second operation as described here is to provide protection from spurious actuations, not protection from operator error. Protection from operator error may involve similar but more restrictive provisions, as addressed in guidance related to Human Factors.*

Observation: This guidance in DI&C-ISG-04 provides acceptable defensive measures that eliminate spurious actuation concerns from operator interface stations.

- *Multidivisional control and display stations should be qualified to withstand the effects of adverse environments, seismic conditions, EMI/RFI, power surges, and all other design basis conditions applicable to safety-related equipment at the same plant location. This qualification need not demonstrate complete functionality during or after the application of the design basis condition unless the station is safety-related. Stations which are not* *safety-related should be shown to produce no spurious actuations and to have no adverse effect upon any safety-related equipment or device as a result of a design basis condition, both during the condition and afterwards. If spurious or abnormal actuations or stoppages are possible as a result of a design basis condition, then the plant safety analyses must envelope those spurious and abnormal actuations and stoppages. Qualification should be supported by testing rather than by analysis alone. D3 considerations may warrant the inclusion of additional qualification criteria or measures in addition to those described herein.*

Observation: This guidance in DI&C-ISG-04 sets the expectations for qualification of NSR digital I&C equipment to prevent spurious actuations or other adverse effects on safety-related equipment or devices as a result of a design basis condition, both during the condition and afterwards. The design basis conditions that should be considered for such qualification testing is not specified; however, it suggests that they are limited to transient conditions by the during and afterwards criteria.

- *Loss of power, power surges, power interruption, and any other credible event to any operator workstation or controller should not result in spurious actuation or stoppage of any plant device or system unless that spurious actuation or stoppage is enveloped in the plant safety analyses.*

Observation: This guidance in DI&C-ISG-04 provides acceptable defensive measures that eliminate spurious actuation concerns from operator interface stations.

- *The design should have provision for an "operator workstation disable" switch to be activated upon abandonment of the main control room, to preclude spurious actuations that might otherwise occur as a result of the condition causing the abandonment (such as control room fire or flooding). The means of disabling control room operator stations should be immune to short circuits, environmental conditions in the control room, etc. that might restore functionality to the control room operator stations and result in spurious actuations.*

Observation: This guidance in DI&C-ISG-04 provides acceptable defensive measures that eliminate spurious actuation concerns from operator interface stations.

- *Failure or malfunction of any operator workstation must not result in a plant condition (including simultaneous conditions) that is not enveloped in the plant design bases, accident analyses, and anticipated transients without scram (ATWS) provisions, or in other unanticipated abnormal plant conditions.*

(Comment 7-3): *The guidance in ISG-04 is insufficient, because:*

(1) There is no discussion of the effects of workstation failures or design defects on intra-division NSR or SR equipment. ISG-04 is limited to inter-division issues.

(2) The guidance for two operator actions is inadequate because it does not address independence for the processing and communication of those actions. Without adequate defensive measures, there are single random hardware failures and single design defects that can erroneously generate the signal (or signals) that would normally result from both actions.

NRC Staff Response to Comment 4-6 and Comment 7-3

The NRC staff understands that the comments are addressing the adequacy and deficiencies of DI&C-ISG-04 with regards to information on defensive measures, considered a subset of what is now referred to as Alternative Methods, to address spurious actuation. First, the NRC staff notes that DI&C-ISG-04 is beyond the scope of the BTP. Section B.3.1.3 of BTP revision 8 allows for the use of NRC-approved alternative methods such as defensive measures to be used to address CCF. The NRC staff agrees with the premise of the comments that applicants could use DI&C-ISG-04 as one source of information to address spurious operation. To the extent applications use DI&C-ISG-04 for alternative methods to address spurious operation , the NRC staff will evaluate the applications on a case-by-case basis. No changes were made as a result of the comments.

Comment No. 4-7

Relevant International Guidance

The Multinational Design Evaluation Programme (MDEP) program has issued two Generic Common Positions that are relevant to the treatment of postulated spurious actuations caused by NSR digital I&C equipment:

- *DICWG No. 10, Version 7, Common Position on Hazard Identification and Controls for Digital Instrumentation and Control Systems*
- *DICWG No. 13, Common Position on Spurious Actuation*

These documents recommend using hazards analyses to assess the vulnerabilities and to credit design attributes that reduce the likelihood or mitigate the consequences of the spurious actuation such that it can be removed from further analysis.

NRC Staff Response

The NRC staff agrees with the comment that the identified MDEP positions are relevant to the treatment of postulated spurious actuations, but the comment does not identify any issue in BTP 7-19 or recommend any specific change to BTP 7-19. The guidance in BTP 7-19 is primarily based on criteria referenced in industry standards incorporated by reference into the Code of Federal Regulations and applicable to U.S. NPPs. However, the NRC staff has considered the knowledge and experience of international regulators and standards organizations when developing Revision 8 of this BTP.

Even though the staff did not modify the document as a result of this comment, the NRC staff continues to engage with international regulators on topics such as DI&C regulatory criteria. Further, the NRC staff that participated in developing DICWG No. 10 and 13 also participated in the development of this revision to the BTP. This revision to the BTP includes refined guidance to provide additional flexibility on the use of design and analytical solutions to address CCF including CCF that results in spurious operation by addressing the likelihood of failure for lower safety significant systems. These refinements include increased focus on discovering and addressing specific vulnerabilities that may lead to CCF. No changes were made as a result of this comment.

Comment No. 4-8

Other Factors to Consider

The issues associated with postulated common cause failures in safety-related digital I&C systems that result in the failure of the safety-related system to act when needed (Condition 1) are fundamentally different than hazards in safety-related and NSR digital I&C control systems that are postulated to cause spurious actuation of safety-related and other important components (Condition 2).

Condition 1 Attributes

- *Regulatory basis is specifically addressed by SRM-SECY-93-087*
- *Concerns are clearly defined as a beyond design basis event*
- *Conditions to be evaluated are well defined as postulated loss of actuation capability due to software CCF coincident with postulated initiating events (i.e., abnormal operation occurrences and postulated accidents)*
- *Well-developed evaluation methodology is available in NUREG/CR-6303 to identify software CCF vulnerabilities of concern*
- *Best-estimate analysis methodologies and acceptance criteria are well understood*
- *Software CCF vulnerabilities of concern can be addressed by familiar and understood design features (e.g., diverse actuation systems or defensive measures) or coping analyses*

Condition 2 Attributes

- *Regulatory basis is not addressed by SRM-SECY-93-087*
- *Regulatory basis for spurious actuation concerns caused by safety-related or NSR digital I&C systems is not well developed and therefore confusing*
- *Concerns are expressed in ways that create confusion regarding their treatment as either design basis conditions or beyond design basis events*
- *Conditions to be evaluated are not well-defined or understood for multiple spurious component actuation scenarios except to be treated as with no other coincident conditions to be assumed*
- *No well-developed hazard evaluation methodology is available to guide the evaluation of spurious actuation concerns caused by postulated safety-related or NSR digital I&C system failures*
- *Use of design basis or best-estimate analysis methodologies and acceptance criteria are not clearly identified for evaluation of the new postulated initiating events*
- *Spurious actuation vulnerabilities of concern are addressed by a less-familiar and understood set of design features*

The goal for the treatment of spurious actuations should be defined and reviewed by the various stakeholder groups. In particular, the acceptability of the defensive measures discussed in DI&C-ISG-04 be confirmed as acceptable solutions. The use of sufficient defensive design measures that can be shown to prevent credible transients that are not bounded by the plant Chapter 15 safety analyses. The most direct approach is to use segmentation of control groups to limit adverse effects along with recognition that these control groups also rely on different signal trajectories and will have non concurrent triggers. The NSR control systems are in continuous operation under the observation of the control room operators. These points are *differentiators from safety-related system designs that have redundancies all relying on signal inputs from the same system parameter that makes them vulnerable to concurrent triggers. This approach would be consistent with the Watts Bar Unit 2 precedent.*

NRC Staff Response

The NRC staff understands the comment to recommend a framework that distinguishes between considerations relevant to a CCF that results in a loss of function and those relevant to a CCF that results in spurious operation. The staff also understands that the comment is questioning the regulatory basis for considering spurious operation for SSCs of varying safety significance. The NRC staff disagrees with the comment. The NRC staff has determined that spurious operation is a potential outcome of CCF originating from latent design defects. Consistent with the Commission's direction in SRM-SECY 93-087, CCFs (originating from latent design defects) that lead to spurious operations are beyond design basis events and, similar to a CCF that results in a loss of function, necessitate specific design or analytical solutions in an application. CCFs resulting from latent design defects are the focus of this BTP, whose regulatory basis is established by SRM-SECY 93-087.

Revision 8 of this BTP provides a reference to DI&C-ISG-04. The examples noted by the comment, such as control function segmentation and non-concurrent triggers, are potential design solutions that can used to address CCF in accordance with the guidance provided in this BTP revision.

No changes were made as a result of this comment.

Comment No. 4-9 and 7-4

Recommendations

(Comment 4-9) *A better way to address the concerns with potential hazards in safety-related and NSR digital I&C control systems that are postulated to cause spurious actuation of safety-related and other important components has five specific actions:*

1. *Remove the applicable guidance from BTP 7-19 Draft Revision 8 (as shown in the attached mark-ups), since it is premature to issue guidance that creates more confusion than it solves regarding the treatment of spurious actuation hazards.*

2. *Clarify the regulatory basis for the treatment of spurious actuation hazards as either design basis or beyond design basis events. It may be useful to couple this regulatory basis issue to Clause 4.h in IEEE Std 603-2018, when it is endorsed.*

3. *Develop a complete and separate set of unambiguous regulatory guidance with a clear compliance framework that is focused on the treatment of hazards in safety-related and NSR digital I&C control systems that are postulated to cause spurious actuation of safety-related and other important components.*

4. *Coordinate the development of the new regulatory guidance documents with other industry stakeholders (e.g., Nuclear Energy Institute) to ensure the guidance is consistent with other industry guidance documents being developed.*

5. *Update the evaluation criteria found in DI&C-ISG-04, Revision 1, Section 3, Multidivisional Control and Display Stations, and Standard Review Plan Section 7.7, Revision 6, with the new regulatory guidance developed for the treatment of hazards in safety-related and NSR digital I&C control systems that are postulated to cause spurious actuation of safety-related and other important components.*

This approach would provide the clarity in the promulgation of a new regulatory guidance document focused on the treatment of hazards in safety-related and NSR digital I&C control systems that are postulated to cause spurious actuation of safety-related and other important components in an unambiguous and complete manner within a clear compliance framework.

(Comment 7-4, responding to Comment 4-9, Action Item No. 1, above) Spurious operations are a serious threat to plant safety due to the ever-increasing extent of digital integration. Raising awareness to these issues in BTP 7-19, including the distinction in analysis methods for spurious operations due to random hardware failures and design defects, is guidance that industry needs in the short term. In the future, the Staff should provide additional more comprehensive guidance to address defensive measures that can be credited in preventing *or limiting spurious operations from both of these sources*

<u>NRC Staff Response</u>

The NRC staff has the following responses to these recommendations:

Comment 4-9, Recommendation No.1 and Comment 7-4 The NRC staff understands comment 4-9 to suggest the removal of guidance pertaining to spurious actuation from the BTP. The staff understands comment 7-4 to disagree with this suggestion in comment 4-9 based upon considerations of safety and technical concerns with spurious actuation. With regard to comment 4-9 Recommendation 1, the staff disagrees with the suggestion to remove spurious operation guidance from the BTP. Spurious operation is one potential outcome of a CCF that originates from a latent design defect. These types of spurious operations have the potential to affect multiple different design functions and could place the plant in a condition that cannot be reasonably mitigated. Spurious operations due to latent design defects is a subject of this BTP. The NRC staff agrees with comment 7-4 to the extent that this comment suggests the BTP should include guidance for reviewing spurious operations due to latent design defects. This is because the potential for spurious operation failure modes generally increases with the level of integration and it is important for staff reviewers to confirm whether an application provides adequate defense-in-depth. This BTP revision also included guidance for proposing NRC-approved alternative methods which would include concepts such as defensive measures to address CCFs. The NRC staff made changes to the discussion of spurious operation in response to these comments.

4-9, Recommendation No. 2 The NRC staff agrees with this comment, in part. The BTP was revised to clarify that spurious operation as a result of a CCF (originating from latent design defects) is considered a beyond-design-basis event and is within the scope of this BTP. This is consistent with the Commission's direction in the SRM-SECY 93-087. The BTP was also revised to clarify that spurious operations as a result of design basis events (e.g., single failures) are outside the scope of this BTP. The comment about endorsement of *IEEE Std 603-2018* is beyond the scope of this revision to the BTP.

4-9, Recommendation No. 3 The NRC staff understands this comment to ask for a separate set of guidance for applicants addressing spurious operations, rather than providing staff review guidance in BTP 7-19, Revision 8. The staff does not disagree with the recommendation to develop guidance for applicants; the staff may consider developing such guidance on spurious operation at a later date. However, the BTP was revised to provide guidance for staff review of applications addressing CCF of SSCs with varying safety significance, which includes the assessment of spurious operation originating from latent design defects. This BTP revision also clarifies the regulatory basis for addressing spurious operations as a result of CCF originating from latent design defects and the design and analytical methods for the D3 assessment the staff evaluates in that regard.

4-9, Recommendation No.4 The NRC staff understands this comment to be in the context of developing separate guidance for spurious operations as described in Recommendation number 3 of comment 4-9. At this time, the staff is not developing separate guidance for applicants to address spurious operation but may develop such guidance in the future. The staff will consider the need for additional guidance as suggested, which may include further interaction with the public.

4-9, Recommendation No.5 The NRC staff understands this comment to be in the context of revising the guidance in SRP Section 7.7 and DI&C-ISG-04 for addressing spurious operations rather than the guidance in BTP 7-19, Revision 8. Changes to SRP Section 7.7 and DI&C-ISG-04 are not within the scope of this BTP revision. No changes were made as a result of this comment.

Letter 5—Comments from SunPort

<u>Comment No. 5-1</u>

Section B.3.3.b, Consequences of the CCF Hazard Are Acceptable

Clarification: The discussion refers to evaluating postulated accidents occurring in conjunction with each single postulated CCF to ensure that the plant response calculated using realistic assumptions does not result in 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 acceptance criteria should be clarified to be consistent with other beyond design basis events evaluations.

*Recommendation**:** Reactor coolant integrity should use the same acceptance criteria and that allowed for 10 CFR 50.62 ATWS evaluations: reactor coolant system pressures should not exceed ASME Service Level C limits). Containment structural integrity should be the same for 10 CFR 50.44 as specified in RG 1.7: containment pressures should not exceed ASME Service Level C limits).*

NRC Staff Response

The NRC staff understands the comment to explain that acceptance criteria for BDBE occurring in conjunction with each single postulated CCF events should be normalized, such that there is one generic set of acceptance criteria applicable to all beyond-design-basis events. However, converting the existing acceptance criteria in Section B.3.3.b to a generic set of acceptance criteria for the reactor coolant pressure boundary and containment response limits may not be appropriate for all types of postulated accidents for all types of operating and new reactor plants. Further, not all beyond-design-basis events result in the same consequences and thus these events do not necessarily have the same acceptance criteria. This is due to differences in regulatory treatment, probability of occurrence, and different types of design features that may be credited for responding to post-event containment static and dynamic loading.

Acceptance criteria for plant responses to different types of accident events are currently presented in different sections of the SRP and in other NRC guidance documents. Licensees already have flexibility in their existing design bases analysis regarding the establishment of plant-specific acceptance criteria. Applicants and licensees are encouraged to engage the NRC staff during pre-application meetings and may propose alternative acceptance criteria when a design is submitted for staff review. Generic acceptance criteria for beyond design basis events is beyond the scope of the BTP and this comment response document. BTP 7-19, Revision 8, was not changed as a result of this comment.

Comment No. 5-2

Section 5.2, IEEE Std 603-1991 Applies

Item b. says "For an A1 system, potential spurious operation of safety-related components or components that are NSR ..." An A1 system has no NSR components.

Recommendation: Revise to say "For an A1 system, potential spurious operation of safety-related components due to CCF hazards ..."

NRC Staff Response

The comment is pointing out a potential error in the draft BTP. The NRC staff agrees with the comment. However, the specific text referenced by the comment has been moved and revised in response to other comments. No other changes were made as a result of this comment.

Comment No. 5-3

Section 5.2, IEEE Std 603-1991 Applies

Item c.3.ii says: "For highly-integrated B1 systems (e.g., distributed control systems), the application should demonstrate that potential spurious operation of multiple functions is bounded by the accident analysis." SRP 7.7 R6 says "The evaluation of multiple independent failures is not intended." Are these two documents consistent? (Underlining added)

Recommendation: Clarify whether the two documents are consistent with respect to multiple failures.

NRC Staff Response

The comment is asking whether there is an inconsistency between the draft BTP and SRP Section 7.7. The referenced documents are consistent. The text in question from the BTP specifically refers to “highly-integrated” SSCs and provides an example of a distributed control system in a non-safety-related context (i.e., a B1 system, as designated in draft BTP 7-19, Rev. 8, for comment). An NSR system is not subject to independence requirements. If the proposed NSR system has “highly-integrated” functions on the same distributed control system, then the functions are not independent. Accordingly, a CCF within this same platform can result in a spurious operation of multiple functions, and this scenario does not represent “multiple independent failures.” The evaluation of the NSR system is unlike that of the safety-related system, in which functions are independent and multiple independent failures need not be considered. In addition, the specific text referenced by the comment has been moved and revised in response to other comments. No changes were made as a result of this comment.

Comment No. 5-4

Section 8.1, System Representation as Blocks

The document says: “Diversity is determined at the block level.”

Recommendation: It would be better to say: “Diversity is evaluated at the block level.”

NRC Staff Response

The NRC staff agrees with this comment. The staff revised BTP 7-19, Revision 8, Section 6.1 to clarify the proper application of systems blocks to represent various portions of the proposed systems in order to accurately demonstrate the architecture of the proposed system when performing a D3 assessment.

Letter 6—Comments from Mr. Yu

Comment No. 6-1

Evaluation Target

Issue: Inconsistent evaluation target descriptions in this guide title and content.

Details: Evaluation target was described as "CCF hazards due to software" in guide title, and "Diversity and Defense-in-Depth" in guide content.

Suggestions: Add further explanation of evaluation target relevant descriptions and their relationships.

NRC Staff Response

The NRC staff agrees that the title and scope of the draft BTP were inconsistent. The staff modified BTP 7 19, Revision 8, to provide guidance consistent with the title and the scope of the BTP. Specifically, the staff revised the title to “Guidance for Evaluation of Defense in Depth and Diversity to Address Common Cause Failure Due to Latent Defects in Digital Safety Systems.”

Comment No. 6-2

Defense-in-Depth

Issue: There is an unnecessary statement in the last paragraph in "A. BACKGROUND" in this guide. One standard solution may not be applicable to all DI&C systems. Instead we need to express "standard solution", because it makes the system behavior predictable and deterministic, and more safety. In fact, there has been some basic safety principles (standard solution) we must insist on, and the most basic and important of these is "defense-in-depth."

Details: NUREG-0493NUREG/CR-6303 and the previous version of NUREG/BTP 7-19 all described the echelons of defense of DI&C systems in NPP. In addition, those different periods guides described different echelons of defense, so it is necessary to clarify what is the latest understanding and requirements about the echelons of defense of DI&C systems in NPP.

Suggestions: Add further explanation of DI&C systems relevant safety principles, especially "Defense-in-Depth" relevant concepts and how it works in DI&C systems.

NRC Staff Response

The NRC staff agrees in part with this comment. The staff agrees with modifying BTP 7-19, Revision 8, to add explanation on safety principles and echelons of defense, as suggested by the comment. The staff disagrees with adding additional guidance defining the safety principle of “defense-in-depth” because this BTP serves to provide guidance on how the staff should review licensee D3 assessments. A further explanation of defense-in-depth is not within the scope of the BTP. For more detailed information on defense-in-depth staff should refer to NUREG CR-6303.

Comment No. 6-3

Hazard Analysis

Issue: “The spurious operation should be considered as an initiating event without a concurrent DBE”, Stated in "5.2 a" in this guide , however, the above statement is inaccurate and lacks basis.

Details: DBE is an approximate concept, take one of them as an example, there are so many possible situations that can cause the small break loss of coolant accident (SBLOCA), some situation can concurrent with the spurious operation caused by software defect. Spurious operation can initiate DBE, it has already been showed in an nuclear power plant operating event in China, so the spurious operation should be considered as an initiating event with a concurrent DBE, unless you can rule it out with good reason.

Suggestions: Add relevant basis of the above consideration, otherwise the conclusion is not valid.

NRC Staff Response

The NRC staff disagrees with this comment. The comment seems to be asking the staff to evaluate spurious operation as an initiating design-basis event concurrent with another DBE.

The staff would not evaluate two independent failures concurrently if both events were DBEs. Further, the focus of this BTP is beyond design basis events. The Commission has previously determined that CCFs due to latent defects are beyond-design-basis events as stated in the SRM-SECY 93-087. The treatment of spurious operation as a result of CCF as a beyond design basis event is not a decision made in this BTP, but rather a conclusion determined in the SRM-SECY 93-087. This comment does not provide sufficient information for staff to consider the situation described in the details of this comment (i.e., a spurious operation causing a DBE).

No changes were made to the BTP as a result of this comment.

Comment No. 6-4

Graded Approach

Issue: Graded approach in Section B. 2.1 in this guide has little or no sense.

Details: There have been too many words to describe the different system and device depending on the importance of safety in this guide, such as: safety-related system, safety computer system, non-safety, safety divisions, safety features, safety system, non-safety-related systems, safety-related components, safety group, non-safety system, critical safety functions, safety-related DI&C system and so on, so adding more descriptions (safety significant and not safety significant) in section B. 2.1 in this guide, only adds confusion.

Suggestions: Using the sensitivity to CCF and safety-related or not for categorizing DI&C systems.

NRC Staff Response

The NRC staff agrees in part with this comment. The staff agrees that these terms have not been used consistently in the draft BTP. The NRC staff revised BTP 7-19, Revision 8, to ensure that terms are used consistently throughout the guidance.

The NRC staff does not agree with the suggestion to use “sensitivity to CCF” and whether SSCs are safety-related for categorization of DI&C systems, as suggested in the comment. Instead, the staff revised the BTP to more clearly categorize SSCs based on safety significance.

Letter 7—Comments from NAE

Nuclear Automation Engineering, LLC, submitted responses to the comments submitted in Letter 4 of this analysis of public comment for BTP 7-19, Revision 8. The comments in Letter 7 are documented and addressed along with the applicable responses to Letter 4.

Letter 8—Comments from NEI

Comment No. 8-1

Spurious Operations, Section A, Regulatory Basis Section 5

Perspectives on IEEE 603-1991 Clauses 4.8 and 5.6.3

IEEE 603-1991 Clause 4.8 states that "The conditions having the potential for functional degradation of safety system performance and for which provisions shall be incorporated to retain the capability for performing the safety functions (for example, missiles, pipe breaks, fires, loss of ventilation, spurious operation of fire suppression systems, operator error, failure in non-safety-related systems)."

1. *In the example list, the phrase "failure in non-safety-related systems" is not intended to include a software CCF failure mode. Rather, in keeping with the other examples in clause 4.8, the "failure in not-safety-related systems" should be interpreted as spatial proximity hazards to the qualification of nearby safety systems. A latent software defect in a non-safety-related system should not be interpreted as a spatial proximity hazard similar to the other examples listed. The term "failure", as defined in IEEE 379, does not include design deficiencies (i.e., a latent software design error) in the scope. As such, the phrase "failure in not-safety-related systems" should not include software CCFs as a type of failure mode.*

2. *Based on the discussion in 1) above, the phrase "having the potential for functional degradation of safety system performance" should be interpreted in an operational context. Meaning that, if one of the example failures were to occur, the actual function of safety system performance would be challenged, therefore, an operability determination would typically be performed. If a latent software defect did occur in a non-safety-related system, it would not necessarily affect the actual function of safety system performance. The latent software defect may create an unanalyzed condition; however, the unanalyzed condition is not equivalent to a functional degradation of safety system performance.*

Perspectives on SRM-SECY 93-087

SRM-SECY-93-087 refers to DI&C CCF events as a "loss of more than one echelon of defense-in-depth." A spurious operation should not be considered a loss of defense-in-depth nor a loss of the safety function. The current draft of BTP 7-19 does not equate "loss" with "spurious operation". Position 2 in SECY-93-087 states, "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."; whereas BTP 7-19 states, "The spurious operation should be considered as an initiating event without a concurrent DBE." As such, spurious operations should not be analyzed the same way as a latent design error (e.g., latent software defect) that causes a loss of function.

Recommendation

Because IEEE 603-1991, Clauses 4.8 and 5.6.3, do not provide a licensing basis requirement to analyze for spurious operations caused by a software CCF, NEI recommends:

1. Deleting the reference to IEEE 603-1991 in Section A.1 "Regulatory Basis" and the other references to spurious operations throughout the BTP.

2. Moving the guidance in Section 5 "Spurious Operations" from the draft Revision 8 of BTP 7-19 to another NRC guidance document. NEI is very interested in continuing the technical discussion on DI&C and spurious operations. The NRC and the NEI DI&C working group should schedule a public meeting in the near future to clarify the technical details and the appropriate guidance to document the results.

NRC Staff Response

The NRC staff understands the comment's point to be that IEEE Std. 603-1991 clauses 4.8 and 5.6.3 do not include spurious operation caused by software CCF as a type of "failure in non-safety related systems." Also, the NRC staff understands the comment's point to be that an unanalyzed condition is not equivalent to a functional degradation of safety system performance with regard to IEEE Std. 603-1991 clause 4.8. The NRC staff disagrees with this comment's position on Clause 4.8 of IEEE Std. 603-1991, however the staff removed the subject text from the BTP, and therefore the issue no longer needs to be resolved to complete the BTP.

The NRC staff also understands the comment to suggest that the guidance regarding spurious operation in Section 5 of the BTP be removed in its entirety and located in a separate guidance document. In the version of BTP 7-19 published for public comment in January 2020, the guidance on spurious operation was in Section 5 of this BTP; to address this and other public comments the staff removed Section 5, spurious operation. Instead, the NRC staff included the technical content related to spurious operation into Section 3 of the BTP.

The NRC staff declined to adopt this comment's suggestion to remove the guidance regarding spurious operation in its entirety, and instead chose to retain spurious operation guidance in Section 3 of the BTP, which provides guidance on D3 assessments. Due to the ability to integrate different design functions using digital technology (i.e., highly integrated digital systems), it can be challenging to identify CCF vulnerabilities and evaluate potential consequences of postulated spurious operation affecting multiple different functions due to CCFs resulting from latent defects. Spurious operations due to CCFs (originating from a latent defect in hardware, software, or software-based logic) have the potential to place the plant in a condition that cannot be reasonably mitigated. Therefore, the NRC staff considers retaining this guidance important to ensure that the staff reviewers can reach a finding regarding whether overall defense-in-depth of the plant is maintained for a proposed design. Although not related to the BTP, the comment encourages continued technical discussion among stakeholders and the staff on spurious operation, and the staff agrees such discussion would be useful.

Comment No. 8-2
Design Attributes, Section 3.1

Section 3.1, entitled "Means to Eliminate CCF Hazard from Further Consideration" does not explicitly state that the design attributes described in Sections 3.1.1, 3.1.2, and 3.1.3 can be used collectively in eliminating the CCF hazard from further consideration.

In Section 3, entitled "Diversity and Defense-in-Depth (D3) Assessment" at the end of the first paragraph it notes that "...the results of the D3 assessment should show that vulnerabilities to CCF hazards have been adequately addressed through any combination of the following:"

Similar language should be used in Section 3.1 to clarify that a combination of design attributes (Sections 3.1.1, 3.1.2, and 3.1.3) can be used in determining that the CCF hazard has been eliminated from further consideration.

Recommendation

Reword the 1st sentence in the last paragraph of Section 3.1 to read:

"If the application demonstrates that the use of these design attributes, in any combination or on their own, for an A1 system or component meet the criteria within this BTP, the CCF hazard has been eliminated from further consideration."

NRC Staff Response

The NRC staff agrees with this comment. The staff adopted the proposed change with minor editorial differences.

Comment No. 8-3

DI&C Categorization, Section B.2.1, Table 2-1

The definitions for the A1 – B2 categories need to be clarified to ensure predictable outcomes:

A1 Category:
Regarding the statement "...if not mitigated by other A1 systems." Is there an inherent assumption that the A1 systems normally relied upon for mitigation are not available or do not function? If so, one could postulate unacceptable consequences for practically any accident "if [the accident is] not mitigated by other A1 systems."

B1 and B2 Categories:
Does the term "consequences to plant safety" refer to dose consequences as it clearly does for A1 systems?

B1 Category:
Regarding the statement "Directly changes the reactivity or power level..." There are many balance of plant SSCs that can directly change the secondary side of the plant and affect reactivity and reactor power level, but would not be considered safety significant.

Vertical Category Descriptions

The labels of "Safety Significant" and "Not Safety Significant" are not appropriate given the deterministic and qualitative definitions provided in each of the four categories. The qualitative definitions may describe varying levels of safety from a DI&C deterministic perspective, but they do not describe safety significance from a risk-informed (i.e., RG 1.174) perspective. If the labels of "Safety Significant" and "Not Safety Significant" remain, it will cause confusion in the categorization process and challenge current efforts to embrace a more risk-informed approach to licensing and oversight functions.

Recommendation

See suggested revision to Table 2-1 at the end of this comment table for more detail.

1. *Reword the 2nd deterministic definition under A1 to read "Failure could directly lead to accident conditions that may cause unacceptable consequences (i.e., exceeds siting dose guidelines for a DBE) and no other A1 systems are able to provide the safety function."*

2. *Incorporate the second paragraph after Table 2-1 (starts off with “Risk insights in terms of...”) into Table 2-1 such that it is clearly part of the categorization process. This change would justify the vertical labels of “Safety Significant” and “Not Safety Significant”; otherwise the labels would be misleading because the deterministic definitions do not effectively characterize safety significance.*

3. *Revise the part of the 1st definition under B1 to read “Directly changes the reactivity or power level of the reactor that could initiate an accident sequence...” Another approach could be to note that some changes (e.g., a change in steam demand for a PWR) is an indirect effect on reactor power level and reactivity. This would preclude any failure of a balance of plant (BOP) component that causes a minor increase (or decrease) in the secondary side to be considered safety significant.*

4. *Revise the 2nd definition under B1 and B2 to remove the phrases that refer to “consequences” and replace it with the concept of an “impact” on plant safety.*

	Safety-Related	*Non-Safety-Related*
Safety Significant* *A significant contributor to plant safety*	***A1 DI&C SSCs*** *Relied upon to initiate and complete control actions essential to maintain plant parameters within acceptable limits established for a DBE.* ***or*** *Failure could directly lead to accident conditions that may cause unacceptable consequences (i.e., exceeds siting dose guidelines for a DBE) and no other A1 systems are able to provide the safety function.* ***Application should include a D3 assessment as described in Section B.3***	***B1 DI&C SSCs*** *Directly changes the reactivity or power level of the reactor that could initiate an accident sequence or affects the integrity of the safety barriers (fuel cladding, reactor vessel, or containment).* ***or*** *Failure ~~may result in unacceptable consequences to~~ has a high impact on plant safety due to integration of multiple control functions into a single system.* ***Application should include a qualitative assessment as described in Section B.4***
Not Safety Significant* *Not a significant contributor to plant safety*	***A2 DI&C SSCs*** *Provides an auxiliary or indirect function in the achievement or maintenance of plant safety.* ***Or*** *Maintains the plant in a safe shutdown state after the plant has reached initial safe shutdown state.*[9] ***Application should include a qualitative assessment as described in Section B.4***	***B2 DI&C SSCs*** *Does not have a direct effect on reactivity or power level of the reactor or affect the integrity of the safety barriers (fuel cladding, reactor vessel, or containment).* ***And*** *Failure does not ~~have consequences to~~ impact plant safety or whose failure can be detected and mitigated with significant safety margin.* ***Application may need to include a qualitative assessment as described in Section B.4*** *if the proposed design could introduce conditions*[10] *that have not been previously analyzed in the SAR.*

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

NRC Staff Response

NRC Staff response to "The definitions for the A1 – B2 categories need to be clarified to ensure predictable outcomes"

The comment raises clarifying questions on categories A1, B1, and B2 on Table 2-1. The specific text referenced by the comment has been moved and revised in response to this and other comments. Specifically, the staff revised the BTP to remove Table 2-1 as well as the SSC categorization designators, A1, A2, B1, and B2, as part of edits to revise the safety-significance determination scheme. Because of this revision, the SSC safety significance descriptions were edited for additional clarity. No other changes were made as a result of these comments.

NRC Staff response to "Vertical Category Descriptions"

The NRC staff understands the comment's point to be that the vertical category labels on Table 2-1 are not appropriate as they do not convey a risk-informed perspective. The staff agrees with this comment in part and revised the acceptance criteria in Section 2 for SSC safety significance determinations to provide review guidance on an applicant's potential use of risk insights to inform such determinations. Note that the specific text referenced by the comment has been revised in response to other comments. Consequently, the staff removed Table 2-1 from the BTP and the categorization designators. No other changes were made as a result of this comment.

NRC Staff response to "Recommendation"

To resolve the above substantive comments, the comment suggested four edits to Table 2-1, and included a markup of the table. Because the specific text referenced by the comment has been moved and revised in response to other comments, Table 2-1 was removed from the BTP. Therefore, the staff did not incorporate the recommendations for this table. However, the staff agrees with the comment and considered suggested edits when revising the descriptions of the SSC for the safety-significance determination scheme provided in Section 2 of this BTP. This includes inclusion of risk insights into the Section 2 acceptance criteria. No other changes were made as a result of the comment.

Comment No. 8-4

Software vs. Hardware CCF, Section A, Background, Purpose

The very last sentence of the first paragraph of the Background section states "This BTP is focused on addressing CCF hazards resulting from systematic faults caused by latent defects in software or software-based logic."

CCF due to hardware is mentioned earlier in the paragraph, however the last sentence indicates that CCF due to hardware is not being addressed by this document.

In the Purpose section, second paragraph, fourth sentence states: "However, in integrated DI&C systems, a single random hardware failure can have cascading effects, similar to a CCF hazard (e.g., loss of multiple functions within a safety group, or spurious operation of functions within multiple safety groups). Single random hardware failures with cascading effects are considered DBEs, because random hardware failures are expected during the life of the facility."

Two comments on the above statement:

1. *Earlier in the document it was stated that CCF was considered "beyond design basis". This statement seems to contradict that earlier statement by now suggesting this postulated CCF hazard is not beyond design basis.*

2. *This statement seems to be addressing hardware whereas an earlier statement in the Background section of the document indicated that BTP 7-19 focuses only on systematic errors due to software or software-based logic.*

Recommendation

NEI recommends limiting the scope of BTP 7-19 to just software CCF and remove any discussion regarding hardware and or systems CCF.

<u>NRC Staff Response</u>

The NRC staff agrees, in part, with this comment, and has made changes to clarify the points of potential contradiction raised by the comment regarding whether CCFs are DBEs or BDBEs. However, the NRC staff does not agree that the scope of BTP 7-19 should be limited to software CCF. Further, the NRC staff decided to add the term "design" to "latent defect,"—i.e., to use the term "latent design defect,"—to better reflect the scope of this BTP. Latent design defects can reside in either hardware or software and the scope of the BTP was refined to include consideration of CCF due to latent design defects in hardware, software, and software-based logic. The staff also made conforming changes in the BTP to ensure consistency with the scope refinement. No further changes were made based upon this comment.

<u>Comment No. 8-5</u>

<u>Justification for Not Correcting Specific Vulnerabilities, Section 8.6</u>

Revision 4 of BTP 7-19 contained guidance that would accept system vulnerability to certain beyond design basis events (i.e., common-mode failure in the protection system affecting the response to large-break loss-of-coolant accidents and main steam line breaks). This interpretation has been previously used in licensing actions. This acceptance was based upon the provision of primary and secondary coolant system leak detection, and pre-defined operating procedures that together enable operators to detect small leaks and take corrective actions before a large break occurs. In effect, the vulnerabilities were judged to be acceptably mitigated based on manual operator actions with a recognition that a best-estimate treatment of these beyond design basis event scenarios accepted that they would evolve over time rather than occurring as instantaneous double-ended guillotine breaks (as analyzed in Chapter 15).

BTP 7-19 should be revised to specifically allow the previously accepted resolution of software CCF in the protection system affecting the response to large-break loss-of -coolant accidents and main steam line breaks based on the provision of primary and secondary coolant system leak detection, and pre-defined operating procedures that together enable operators to detect small leaks and take corrective actions before a large break occurs. This mitigation strategy would be used in lieu of more in-depth human factors evaluation of manual operator actions or the addition of diverse actuation features to address instantaneous double-ended breaks coincident with postulated a protection system CCF.

Recommendation

Recommend changing Section 8.6 to read:

8.6. Justification for Not Correcting Specific Vulnerabilities

"Justification should be provided for not correcting any identified vulnerabilities not addressed by other aspects of the application such as design attributes, defensive measures, or provision of alternate trip, initiation, or mitigation capability. This includes any NRC-approved credited operator action taken to prevent the AOO or postulated accident from occurring. These justifications will be reviewed on a case-by-case basis. For example, the use of primary and secondary coolant system leak detection and pre-defined operating procedures that collectively enable operators to detect leaks and take corrective actions before a large break develops. This mitigation strategy would be used in lieu of more in-depth human factors evaluation of manual operator actions or the addition of diverse actuation features to address instantaneous double-ended breaks coincident with a postulated protection system software CCF."

<u>NRC Staff Response</u>

The NRC staff agrees with the comment to allow for more flexibility for the potential use of leak detection and operator actions to prevent AOOs or postulated accidents. However, the staff identified two reasons why the proposed changes to BTP 7-19, Revision 8, are not appropriate. First of all, the staff has not generically determined that the use of primary and secondary coolant system leak detection and pre-defined operating features will be acceptable for all plant configurations and potential events. In its evaluation of this comment, the staff identified several site-specific design characteristics that would have to be addressed on a site-specific basis in the D3 assessment. Therefore, a generic approval is not appropriate. The second reason is that a human factors evaluation should be performed to credit operator actions for preventing the AOO or postulated accident. Based on this comment, the staff provided additional clarifications in Section 6.5 of the BTP 7-19 to provide for the possibility of crediting leak detection and to verify on a case-by-case basis that an adequate technical basis is provided in the application to justify not correcting any identified vulnerabilities.

<u>**Comment No. 8-6**</u>

<u>*Quality of NSR equipment, Section B.3.2.1, Section B.3.2.2*</u>

Second paragraph states:

"For existing systems that are NSR, the quality of these systems should be similar to systems required by the ATWS rule (i.e., 10 CFR 50.62), as described in the enclosure of Generic Letter 85-06." This is a new requirement. In past cases feedwater systems have been used as a credited existing system, which may not have similar quality characteristics.

In Revision 7 of BTP 7-19, Section 3.4 stated:
"Other systems that are credited in the analysis that are in continuous use (e.g., the normal RCS inventory control system or normal steam generator level control system) are not required to be upgraded to the augmented quality discussed above."

In crediting existing NSR systems (3.2.1), to include equipment used to perform credited manual operator actions (3.2.2), continuously operating equipment should not be required to meet the augmented quality standard. For non-continuously operating NSR equipment (i.e., stand-by equipment,) it should be sufficient to provide evidence of reliability (i.e., data and operational experience) to substantiate that the system will perform its intended function when demanded. Evidence of reliability can be used to meet any expectation of "sufficient quality" for non-safety-related systems.

Recommendation

Replace the entire last (2nd) paragraph in Section 3.2.1 and the 3rd and 4th sentences in the first paragraph in Section 3.2.2 (begins with "If the equipment used..." and ends with "Generic Letter 85-06") with:

"NSR systems that are credited in the analysis that are in continuous use (e.g., the normal RCS inventory control system or normal steam generator level control system) are not required to be meet any augmented quality standards. NSR systems that are credited in the analysis that are not in continuous use (i.e., standby,) reliability data and operational experience can be used to conclude that the system will perform its intended function(s) when demanded"

NRC Staff Response

The NRC staff agrees with this comment. The staff adopted the proposed change with some minor editorial differences.

Comment No. 8-7

Tech Specs, Section 3.1.1

Last paragraph of 3.1.1 states:

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

It is not clear how a software CCF could be a factor in the Technical Specification allowable time for a division to be bypassed.

Recommendation

Provide the appropriate link to the Regulatory Basis section and a clarifying example of how an allowable time would be restricted.

NRC Staff Response

The NRC staff agrees with this comment. The NRC staff removed the quoted text from BTP 7-19, Revision 8. The acceptance criterion in Section B.3.1.1.f of the BTP addresses the use of periodic surveillance criteria to verify continued functionality of the diverse portion of the system. No further changes were made as a result of this comment.

Comment No. 8-8

Robust Design Process, Section A.4

The second paragraph of the section titled "Purpose" starts by stating:

"This BTP is intended to address an applicant's approach to address CCF hazards caused by latent defects in the software or software-based logic. This type of CCF hazard is considered a beyond-design-basis event for structures, systems, and components (SSCs) that employ a robust design process to reduce the likelihood of design defects."

The way the 2nd sentence above is constructed could led one to assert that if a "robust design process" was not employed, then the software CCF hazard would no longer be considered a beyond design basis event.

Recommendation

Recommend changing the second paragraph to read:

"This BTP is intended to address an applicant's approach to address CCF hazards caused by latent defects in the software or software-based logic, which are considered beyond-design-basis events."

NRC Staff Response

The NRC staff agrees with this comment. The staff adopted the proposed change with some minor editorial differences. The NRC staff also clarified the scope of the BTP to include consideration of CCF for hardware, software, and software-based logic applications.