March 12, 2020

Office of Administration
Mail Stop: TWFN-7-A60M
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

Subject: Industry Comments on Draft Revision 8 to Branch Technical Position (BTP) 7-19, "Guidance for Evaluation of Common Cause Failure Hazards Due to Latent Software Defects in Digital Instrumentation and Control Systems;" 85 FR 2152-2153; Docket ID NRC-2019-0253

Project Number: 689

Dear Ms. Jennifer Borges:

The Nuclear Energy Institute (NEI)[1], on behalf of its members, submits the following comments on the draft Revision 8 to Branch Technical Position (BTP) 7-19, "Guidance for Evaluation of Common Cause Failure Hazards Due to Latent Software Defects in Digital Instrumentation and Control Systems." We are supportive of the effort to revise this BTP and appreciate the opportunity to comment on the draft revision.

The NEI Digital Instrumentation and Control (DI&C) working group has been actively engaged with the staff in the revision to BTP 7-19 over the past year. The public meetings held during 2019 and into 2020 have been great opportunities to share technical and regulatory perspectives. Overall the NEI DI&C working group is pleased to see how this BTP revision has incorporated a graded approach into the DI&C categorization process and the techniques used to prevent and mitigate a software common cause failure (CCF) hazard.

Please find the attached comments on the current draft Revision 8 to BTP 7-19. Our intention is to provide recommendations, with sound technical and regulatory bases, that clarify the guidance to ensure both licensees and the NRC staff have a common understanding when submitting and reviewing a DI&C license amendment request (LAR.) As stations begin to consider plant modernization, we believe that it is this common understanding that will allow future digital modifications to be reviewed, approved, and implemented in an efficient and predictable manner.

Please contact me at sjv@nei.org and (202) 739-8163 if you have any questions or concerns.

Sincerely,

[1] The Nuclear Energy Institute (NEI) is responsible for establishing unified policy on behalf of its members relating to matters affecting the nuclear energy industry, including the regulatory aspects of generic operational and technical issues. NEI's members include entities licensed to operate commercial nuclear power plants in the United States, nuclear plant designers, major architect and engineering firms, fuel cycle facilities, nuclear materials licensees, and other organizations involved in the nuclear energy industry.

STEPHEN J. VAUGHN
Senior Project Manager, Engineering and Risk

1201 F Street, NW, Suite 1100
Washington, DC 20004
P: 202.739.8163

sjv@nei.org
nei.org

NUCLEAR ENERGY INSTITUTE

March 12, 2020

Office of Administration
Mail Stop: TWFN-7-A60M
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

Subject: Industry Comments on Draft Revision 8 to Branch Technical Position (BTP) 7-19, "Guidance for Evaluation of Common Cause Failure Hazards Due to Latent Software Defects in Digital Instrumentation and Control Systems;" 85 FR 2152-2153; Docket ID NRC-2019-0253

Project Number: 689

Dear Ms. Jennifer Borges:

The Nuclear Energy Institute (NEI)[1], on behalf of its members, submits the following comments on the draft Revision 8 to Branch Technical Position (BTP) 7-19, "Guidance for Evaluation of Common Cause Failure Hazards Due to Latent Software Defects in Digital Instrumentation and Control Systems." We are supportive of the effort to revise this BTP and appreciate the opportunity to comment on the draft revision.

The NEI Digital Instrumentation and Control (DI&C) working group has been actively engaged with the staff in the revision to BTP 7-19 over the past year. The public meetings held during 2019 and into 2020 have been great opportunities to share technical and regulatory perspectives. Overall the NEI DI&C working group is pleased to see how this BTP revision has incorporated a graded approach into the DI&C categorization process and the techniques used to prevent and mitigate a software common cause failure (CCF) hazard.

Please find the attached comments on the current draft Revision 8 to BTP 7-19. Our intention is to provide recommendations, with sound technical and regulatory bases, that clarify the guidance to ensure both licensees and the NRC staff have a common understanding when submitting and reviewing a DI&C license amendment request (LAR.) As stations begin to consider plant modernization, we believe that it is this common understanding that will allow future digital modifications to be reviewed, approved, and

[1] The Nuclear Energy Institute (NEI) is responsible for establishing unified policy on behalf of its members relating to matters affecting the nuclear energy industry, including the regulatory aspects of generic operational and technical issues. NEI's members include entities licensed to operate commercial nuclear power plants in the United States, nuclear plant designers, major architect and engineering firms, fuel cycle facilities, nuclear materials licensees, and other organizations involved in the nuclear energy industry.

implemented in an efficient and predictable manner.

Please contact me at sjv@nei.org and (202) 739-8163 if you have any questions or concerns.

Sincerely,

Stephen Vaughn

cc: Mr. Eric Benner, NRR
Mr. Wendell Morton, NRR
Ms. Tekia Govan, NRR
Mr. Michael Waters, NRR
NRC Document Control Desk

NEI DI&C Working Group Comments on BTP 7-19, Revision 8

Topic and Affected Section(s)	Comment / Basis	Recommendation
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*	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.

Topic and Affected Section(s)	Comment / Basis	Recommendation
	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. <u>Perspectives on SRM-SECY 93-087</u> 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.	

Topic and Affected Section(s)	Comment / Basis	Recommendation
2. <u>Design Attributes</u> 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.	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.*"
3. <u>DI&C Categorization</u> Section B.2.1 Table 2-1	<u>The definitions for the A1 – B2 categories need to be clarified to ensure predictable outcomes</u>: 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:	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

Topic and Affected Section(s)	Comment / Basis	Recommendation
	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. <u>Vertical Category Descriptions</u> 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.	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 removed the phrases that refer to "consequences" and replace it with the concept of an "impact" on plant safety.
4. <u>Software vs. Hardware CCF</u> 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*	NEI recommends limiting the scope of BTP 7-19 to just software CCF and remove any discussion regarding hardware and or systems CCF.

Topic and Affected Section(s)	Comment / Basis	Recommendation
	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.	

Topic and Affected Section(s)	Comment / Basis	Recommendation
5. Justification for Not Correcting Specific Vulnerabilities Section 8.6	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.	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."

Topic and Affected Section(s)	Comment / Basis	Recommendation
6. <u>Quality of NSR equipment</u> Section B.3.2.1 Section B.3.2.2	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.	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"*

Topic and Affected Section(s)	Comment / Basis	Recommendation
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.	Provide the appropriate link to the Regulatory Basis section and a clarifying example of how an allowable time would be restricted.
8. Robust Design Process Section A.4	The 2nd paragraph of the section entitled "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.	Recommend changing the 2nd 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."*

NEI DI&C Working Group Comments on BTP 7-19, Revision 8

Recommended Edits to Table 2-1

	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.		