From: VAUGHN, Stephen
To: Govan, Tekia; Morton, Wendell
Subject: [External_Sender] NEI Comments on Draft BTP 7-19 Revision 8 (May 2020 version)
Date: Tuesday, June 23, 2020 11:09:42 AM
Attachments: NEI Comments on BTP 7-19 Revision 8 - 6-23-2020.docx

---

Tekia and Wendell,

Please find the NEI DI&C working group updated comment table regarding the May 2020 draft BTP 7-19, Revision 8. These comments are an update to the feedback NEI provided in March 2020 and are based on the discussions and presentations at the June 2nd ACRS DI&C Subcommittee meeting.

If you have any questions or concerns, please let me know.

Regards,

Steve

STEPHEN J. VAUGHN | *SENIOR PROJECT MANAGER, ENGINEERING AND RISK*
1201 F Street, NW, Suite 1100 | Washington, DC 20004
P: 202.739.8163 M: 202.256.5393
sjv@nei.org

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 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 only, without a concurrent DBE…*" As stated in the draft, spurious operations are not analyzed the same way that a latent design defect that could cause a loss of function is analyzed. The Concept of Spurious Operations was not introduced until 2012 (i.e., Rev 6 of BTP 7-19) Earlier revisions of BTP 7-19 (i.e., Revisions 1 thru 5) did not have the spurious operations guidance and it is not clear what prompted the addition. Because the SRM-SECY 93-087 was issued in 1993, about 19 years prior to Revision 6 of BTP 7-19, it does not seem appropriate to be the basis for the spurious operations guidance. In other regulatory areas (e.g., fire protection) the concept of spurious operations has a clear licensing basis	Because SRM-SECY 93-087, GDC 24, 25, and SRP Section 7.7 do not provide a licensing basis requirement to analyze for spurious operations caused by a latent design defect: 1. Move the spurious operation guidance 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. Because highly integrated NSR systems are of greater concern to the staff (as described on page 31-32 of the BTP), the focus of the discussions should be on NSR SSCs that could directly or indirectly affect reactivity.

Topic and Affected Section(s)	Comment/Basis	Recommendation
	requirement. For example, 10 CFR Part 50, Appendix R, Section III.G.2 describes how fire damage to cabling "…could prevent operation or cause maloperation due to hot shorts, open circuits, or shorts to ground…" These maloperations are described as multiple spurious operations (MSOs) in NEI 00-01, "Guidance for Post-Fire Safe Shutdown Circuit Analysis", which was endorsed in part by RG 1.189, "Fire Protection for Nuclear Power Plants." However, because spurious operations caused by latent design defects in DI&C systems does not have a clear tie to a licensing basis requirement, making a like-for-like comparison to fire protection, as described above, is not justified. Likewise, GDC 24, 25, and SRP Section 7.7 do not provide a regulatory basis for requiring a spurious operations assessment.	
2. <u>DI&C Categorization</u> Section B.2.1 Table 2-1	<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.	1. 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. NOTE: In the text, change "system" to "SSCs" because Table 2-1 categorizes by SSCs, not just systems.

Topic and Affected Section(s)	Comment/Basis	Recommendation
	<u>Use of General Design Criteria (GDC) to Categorize an A1 and B1</u> The GDCs are very high-level and it would be challenging for a user to determine the appropriate level (i.e., "to the extent practical") of diversity required for a particular DI&C SSC. Furthermore, not all of the GDCs mention diversity and some use similar terms that may (or may not) be construed as diversity. The GDCs, in and of themselves, do not distinguish whether a DI&C SSC is safety significant. As such, the GDCs criterion is not an effective tool to identify A1 and B1 SSCs. The technical criterion in A1 and B1, including the risk-insights from site-specific PRAs, effectively captures the set of DI&C SSCs; therefore, the GDCs criterion does not add any additional value.	2. If the 1st option is not pursued, either remove the far-left column of the table or Change the "Safety Significant" and "Not Safety Significant" labels to read "High Impact on Safety" and "Low Impact on Safety" respectively. 3. Delete the criterion from the A1 and B1 categories that states "Equipment required to have diversity to the extent practical, per the GDCs"
3. <u>Software vs. Hardware CCF</u> Section A.1 "Background" Section A.4 "Purpose" Various	The addition of a beyond design basis CCF caused by a latent defect in hardware to the May 2020 version of the draft BTP 7-19 needs to be clarified. 1. The term "latent defect" is not well defined and should be limited to only latent defects in design and should not include downstream processes like fabrication. 2. First sentence in second paragraph in Section A.1 "Background" states "*DI&C systems are composed of both hardware components and logic elements (e.g., software).*" This statement is ambiguous	1. Everywhere in the guidance where the term "latent defect" is used, replace it with "latent design defect" 2. Provide a working definition of "latent design defect" as "Undetected errors in hardware and software functional requirements and design" 3. Revise the first two paragraphs of Section A.4 "Purpose" to read:

Topic and Affected Section(s)	Comment/Basis	Recommendation
	because the interface between hardware and software can create the "logic elements" of the DI&C system. 3. The following sentence states "*Regarding the logic portion, DI&C systems or components can also be vulnerable to a CCF due to latent defects in hardware, software, or software-based logic."* seems to include hardware, software, and software-based logic in determining the logic portion of the DI&C system which contradicts the prior sentence that limits "logic elements" to just software. 4. In the Types of Failure Considerations portion of the "Background" section, the description of the "*Failures to be considered as Beyond Design Basis CCF*" and the first sub-bullet "*CCFs resulting from latent hardware or software defects leading to loss of function*" needs more detail. It is not clear what a "latent defect in hardware" is. In Section A.4 "Purpose" in the second paragraph states "*In this guidance, software includes software, firmware, and logic developed from software-based development systems (e.g., hardware description language programmed devices)."* A similar description needs to be provided to clarify how the term "hardware" should be considered in the guidance so it is clear what a latent design defect in hardware is (and what it is not).	"*This document provides guidance for evaluating any D3 means credited to address vulnerabilities to CCF caused by latent design defects in the DI&C system that can adversely impact the system logic, as well as, the effects of any unmitigated CCF outcomes on plant safety. This BTP also provides staff guidance for reviewing a licensee or applicant's graded approach, if used, to address CCF vulnerabilities in systems of differing safety classification.* *In this guidance, software includes software, firmware, and logic developed from software-based development systems (e.g., hardware description language programmed devices) and hardware includes components that interface with software to support the functional logic of the system. As described above, events associated with this type of CCF vulnerability are considered beyond DBE, in accordance with Commission direction in SRM to SECY 93-087."* In addition, move the above revised wording to the "Background" section under the beyond design basis discussion in the Type of Failure Considerations portion. 4. Change the first sentence in the second paragraph of Section A.1 "Background" to read: "*DI&C system logic is composed of both hardware and software*"

Topic and Affected Section(s)	Comment/Basis	Recommendation
	5. BTP 7-19, since 1997, was focused on "Computer-Based Instrumentation and Control Systems". In other words, this BTP was focused on digital I&C systems, where hardware and software are integrated. This draft now isolates hardware from software causing industry confusion.	
5. Crediting Existing Systems Section B.3.2.1	The last sentence in the second paragraph states "The ATWS system to be credited should (1) be diverse from the proposed DI&C system, (2) has been demonstrated to be highly reliable and of sufficient quality, and (3) be responsive to the AOO or PA sequences using independent sensors and actuators as the proposed DI&C system." The phrase "using independent sensors and actuators" is not consistent with 10 CFR 50.62(c)(1) through 10 CFR 50.62(c)(3). The independence requirement starts at the sensor output and ends at the actuating device, as such an independent sensor is not required.	Modify the phrase "using independent sensors and actuators as the proposed DI&C system." To read "…and is independent (from sensor output to the final actuation device) from the proposed DI&C system."
6. Testing Section 3.1.2.a-c	The guidance in Section 3.1.2.a-c does not align with current industry guidance. Having very similar, yet slightly different language, will cause confusion.	Revise Section 3.1.2.a-c to read: "a) A PDD is not considered susceptible to CCF if the PDD is shown to be deterministic in performance, has documentation of all functional states and all transitions between the functional states, and is testable based on the following criteria: — Testing every possible combination of inputs,

Topic and Affected Section(s)	Comment/Basis	Recommendation
		— For PDDs that include analog inputs, the testing of every combination of inputs shall include the whole operational range of the analog inputs. — Testing every possible executable logic path (this includes non-sequential logic paths). — Testing every functional state transition, and — Test monitoring for correctness of all outputs for every case. b) This testing shall be conducted on the PDD integrated with test hardware representing the target hardware. c)It is possible that PDDs include unused inputs. If those inputs are forced by the module circuitry to a particular known state, those inputs can be excluded from the "all possible combinations" criterion."
7. Independent and Diverse Various sections	Throughout the BTP the phrase "independent and diverse" is used in the context of manual system actuations. The term "independent" can have multiple interpretations, which can cause confusion. NEI believes that it is "functional" independence, not electrical isolation independence as described in IEEE 603, that is the intended meaning of the term "independent" when used in the context manual system actuations.	Throughout the BTP where the phrase "independent and diverse" is used in the context of manual system level actuations, replace it with "functionally independent and diverse"
8. NUREG/CR-6303 and 7007	Listing NUREG/CR-7007 as an acceptance criterion is inconsistent with the statement made in Section A.2 that states: "While this NUREG describes a method for quantitatively assessing the amount of diversity in a	Modify the first sentence of Section 3.1.1.b to read:

Topic and Affected Section(s)	Comment/Basis	Recommendation
Section 3.1.1.b Under "Acceptance Criteria"	system, this method has not been benchmarked and should not be used as the sole basis for justifying adequate diversity." To date, the NRC has not required applicants to demonstrate compliance to NUREG-CR-7007.	"*An analysis demonstrates that adequate diversity has been achieved between the diverse portions of the system or component (e.g. NUREG/CR-6303.)*"

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