NEI DI&C Working Group Comments on BTP 7-19, Revision 8 in support of the 2/11/2020 Public Meeting

Topic and Affected Section(s)	Comment/Basis	Recommendation
1. Spurious Operations Section A Regulatory Basis Section 5	Table 1 – Spurious Operations (starting on page 7 has a high-level overview) Perspectives on IEEE 603-1991 Clauses 4.8 and 5.6.3 IEEE 603-1991 Clause 4 is about what, as a minimum, must be documented in the design basis. Clause 4.8 in particular is about conditions (hazards) that could degrade the safety system but provisions are provided so the safety system can perform its safety functions. Clause 5.6.3 requires that safety systems can perform in the presence of the conditions identified in 4.8. In 4.8, what must be documented in the design basis is the set of hazardous conditions that (a) could degrade the safety system and (b) there are provisions incorporated to retain the capability to perform the safety function. It is clear the safety system does not have to prevent the conditions. Rather, the safety system would be designed with provisions so it will continue to perform the safety function. Again, 4.8 is about what must be in the design basis. It appears that the text in the draft BTP 7-19 is requiring evaluations of conditions that might not be in the design basis.	Because licensing basis evidence that spurious operations caused by a beyond design basis event (i.e., software CCF) is a licensing basis requirement per IEEE 603-1991, the spurious operations guidance proposed for Revision 8 to BTP 7-19 should be removed and placed in another NRC guidance document.

NEI DI&C Working Group Comments on BTP 7-19, Revision 8 in support of the 2/11/2020 Public Meeting

Topic and Affected Section(s)	Comment/Basis	Recommendation
2. 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 steam demand 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	NEI recommends two options. Option #1 – 1. Clarify the deterministic definitions in each of the four categories (A1 thru B2). 2. Remove the vertical labels of "Safety Significant" and "Not Safety Significant." 3. 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. For example, the Section 2.1 process could have various steps (i.e., step 1 – use Table 2-1 definitions; step 2 – incorporate risk insights; step 3 – make an integrated risk-informed decision) Option #2 – 1. Remove the deterministic definitions in A1 thru B2 and replace them with a definition of "safety-significant function" and threshold criteria for what is considered "high" and "low"

Topic and Affected Section(s)	Comment/Basis	Recommendation
	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 in moving to embrace a more risk-informed approach to licensing and oversight functions.	
3. <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 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."*	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
	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.	
4. Justification for Not Correcting Specific Vulnerabilities Section 8.2 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	BTP 7-19 should be revised to specifically allow the previously accepted resolution of common-mode failures 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 guillotine breaks coincident with postulated a protection system CCF.

Topic and Affected Section(s)	Comment/Basis	Recommendation
	instantaneous double-ended guillotine breaks (as analyzed in Chapter 15).	Suggested changes: 8.2. Documentation of Assumptions The application documents any assumptions made to compensate for missing information in the design description materials or to explain interpretations of the analysis guidelines as applied to the system. For example, the design basis assumption of instantaneous double-ended guillotine breaks for large-break loss-of-coolant accidents and main steam line breaks can be replaced with a more realistic treatment for break opening times for the best-estimate evaluations. The use of primary and secondary coolant system leak detection and pre-defined operating procedures that together enable operators to detect leaks and take corrective actions before a large break develops. 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

Topic and Affected Section(s)	Comment/Basis	Recommendation
		case-by-case basis. For example, the use of primary and secondary coolant system leak detection and pre-defined operating procedures that together 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 guillotine breaks coincident with postulated a protection system CCF.
5. Quality of NSR equipment Section B.3.2.1	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.	Modify the sentence to state: "For existing systems that are NSR and not continuously operating, the reliability of these systems should be consistent with licensee design programs and processes."

NEI DI&C Working Group Comments on BTP 7-19, Revision 8 in support of the 2/11/2020 Public Meeting

Table 1 – Spurious Operations

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 LARs) ***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	***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***

		separation and consideration of single random failures are specified. (Clause 5.6.3)			
Note: Protection system safety functions are derived from analysis of specific postulated initiating events in FSAR Chapter 15. These events 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.).			