NEI Comments on Draft Revision to BTP 7-19

Affected Section	Comment/Basis	Recommendation
1. "Review Note"	"Therefore, the individual revision numbers of RGs (except RG 1.97) and years of endorsed industry standards are not shown in this BTP." It isn't clear why RG 1.97 is an exception.	Delete "(except RG 1.97)"
2. A. "Background"	"DI&C systems can be vulnerable to a CCF caused by software errors or software developed logic." The phrase "software development logic" is ambiguous.	Replace "software development logic" throughout the document and replace it with the definition on page 6 (Section A.4 "Purpose")
3. A. "Background"	"A CCF of a DI&C system can also actuate a safety-related function or other design functions without a valid demand. This condition is typically referred to as spurious operation but can be used interchangeably with the term spurious actuation." See Comment #26	See Recommendation #26
4. A.1 "Regulatory Basis"	Regarding all of the listed items, paraphrasing and selecting particular excerpts from IEEE Standards or GDCs can cause confusion.	Only list the GDC and title or IEEE Standard and clause and remove any paraphrasing.
5. A.4 "Purpose"	"In this guidance, software includes software, firmware and logic developed from software-based development systems (e.g., Hardware Description Language Programmed Devices)."	Change sentence to read "In this guidance, software includes software, firmware and logic developed software-based development system (e.g., Hardware Description Language)."

Affected Section	Comment/Basis	Recommendation
6. A.4 “Purpose”	“However, in integrated digital systems, a single random hardware failure can have cascading effects, similar to a CCF (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 design basis events (DBEs) whose plant-level results call for conservative deterministic analysis methods to demonstrate that they are bounded by existing identified AOOs, or have acceptable results for any new or unbounded AOOs that are identified through the analysis. RG 1.53 provides guidance for the deterministic analysis of single failures in safety-related systems. A graded approach to this analysis may be applied to systems that are not safety-related.” The above guidance can confuse the concept cascading effects from a single random hardware failure or software error in a non-redundant control system with assessment of CCF in redundant portions of a safety systems.	Recommend clarifying the language and potentially include references to approved definitions or developing new definitions where appropriate.
7. A.4 “Purpose”	“This BTP also addresses CCFs due to latent software defects that can cause spurious operation of a safety or non-safety function that could put the plant in an unanalyzed condition or a condition that cannot be mitigated by a safety-related I&C system. This BTP provides criteria for analyzing such conditions.” See Comment #26	See Recommendation #26

Affected Section	Comment/Basis	Recommendation
8. B.1.1 "Four CCF Positions and Clarifications"	"The term "best-estimate methods" in Position 2 is now referred to as methods using "realistic assumptions," which are defined as the initial plant conditions corresponding to the onset of the event being analyzed." The phrase "is now referred to as" does not provide a reference or justification to substantiate the new clarification.	If the phrase "realistic assumptions" is to be synonymous with "best-estimate methods" provide a reference.
9. B.1.1 "Four CCF Positions and Clarifications"	"…which are defined as the initial plant conditions corresponding to the onset of the event being analyzed." Previous D3 analyses reviewed and accepted by NRC included the following additional aspects of best estimate methods: no concurrent single failures, no concurrent LOOP for postulated accidents, nominal reactivity feedback parameters, and credit for beneficial control system actions.	These aspects should be included in the description of best estimate methods.

Affected Section	Comment/Basis	Recommendation
10. B.1.1 "Four CCF Positions and Clarifications"	"…is based on the NRC concern that software-based or software logic-based DI&C systems development errors are a credible source of CCF. Generally, DI&C systems cannot be proven to be error-free from a design and software development perspective. Therefore, DI&C systems are considered vulnerable to CCF because either 1) identical copies of the software or software-based logic are present in redundant divisions of safety-related systems; or 2) there exists integration of previously separate functions into a single DI&C system. Also, some errors, such as those labeled as "software errors," actually result from errors in the higher-level requirements specifications, in which the system design misrepresent the actual process." How can software-based DI&C system development errors be a beyond design basis event AND a credible source of CCF? The term "error-free" is not appropriate. No system, analog or digital, can be proven to be error-free. Regarding "…some errors, such as those labeled as "software errors," actually result from errors in the higher-level requirements". The same case can be made for analog systems.	Change paragraph to read "…is based on the NRC concern that software-based or software logic-based DI&C systems development errors are a potential source of CCF. DI&C systems are considered vulnerable to CCF because either 1) identical copies of the software or software-based logic are present in redundant divisions of safety-related systems; or 2) there exists integration of previously separate functions into a single DI&C system. Also, some errors, such as those labeled as "software errors," can result from errors in the higher-level requirements specifications, in which the system design misrepresents the actual process."
11. B.1.2 "Critical Safety Functions"	"Therefore, a safety function identified in the plant safety analysis may not always be a critical safety function." This sentence on its own without any additional information is confusing.	Either delete the sentence or provide some additional language to communicate why the statement was made or how to apply the statement.

Affected Section	Comment/Basis	Recommendation
12. B.2.1 "Graded Approach for Categorizing DI&C Systems"	Regarding Table 2-1, Categorization Scheme for Implementing A Graded Approach to Address CCF. The terms "Safety Significant" and "Not Safety Significant" do not effectively describe the threshold between A1 to A2 and B1 to B2.	Recommend changing "Safety Significant" to "High Safety Significant" and "Not Safety Significant" to "Low Safety Significant"
13. B.2.1 "Graded Approach for Categorizing DI&C Systems"	The qualitative definitions for each category A1 through B2 only provide a deterministic approach to categorization and can introduce subjectivity to the categorization process. The safety significance category determination should be an integrated decision-making process and incorporate both deterministic and risk-informed insights.	Recommend adding the following guidance to section B.2.1 to allow licensees to leverage risk-informed insights. "Risk insights from site-specific Probabilistic Risk Assessments (PRAs) used to support risk-informed licensing actions (e.g., 50.69) and/or risk-informed oversight functions (e.g., 50.65) can be used to support the determination as to whether a system, function, or component is high or low safety significant."
14. B.2.1 "Graded Approach for Categorizing DI&C Systems"	"maintains the plant in a safe shutdown state after the plant has reached initial safe shutdown state." Safe shutdown (e.g., hot shutdown, cold shutdown) is site-specific.	Recommend adding a note to highlight that the "safe shutdown" definition depends on the site-specific licensing and design bases.

Affected Section	Comment/Basis	Recommendation
15. B.2.1 "Graded Approach for Categorizing DI&C Systems"	"that directly affects the reactivity or power level of the reactor, or affects the integrity of the safety barriers (fuel cladding, reactor vessel, or containment);" "Affects reactivity" can be almost any balance, primary or secondary, system that affects pressure, temperature, or flow because of core reactivity feedback effects. Examples include condensate booster pumps whose failure typically results in a plant down power from 100%, feedwater heaters whose isolation or other faults may inject colder water and thus increase plant power levels, etc. "Controls reactivity" would encompass rod control system and PWR boron/dilution control. These control system failures are addressed within the analyzed AOOs.	Recommend clarifying what reactivity affects should be considered in B1 systems.
16. B.2.2 "CCF Assessment Commensurate with Level of Integration and Interconnectivity"	"However, it is still necessary to ensure that CCFs occurring within or among the systems in the other categories do not result in the plant being put into a new unanalyzed state." The guidance does not provide boundaries for which systems need to be considered or the types of events that need to be considered in those undefined systems. Overall it is not clear how the level of integration or interconnectivity is measured or where the lines should be drawn.	Clear boundaries for level of integration and interconnectivity need to be articulated so that a D3 assessment for an A1 system licensing action does not introduce scope creep in the review.

Affected Section	Comment/Basis	Recommendation
17. 3 “D3 Assessment”	“These three measures are the performance of a D3 assessment, the use of defensive design measures to avoid or tolerate faults, and pre-planned actions and provisions to cope with unanticipated hazards or reactor conditions.” The expansion of the D3 assessment definition beyond what is described in NUREG/CR-6303 can create confusion. The identification of defensive measures to be credited and the associated justification should be linked to NUERGE/CR-6303 assumption guidance in Section 6. The treatment of spurious component actuations do not readily fit the evaluation methodology in NUREG/CR-6303 (see defined failure types in Section 3.3). The treatment of non-safety control system 'CCFs' does not fit the block evaluation guidance in NUREG/CR-6303 (see Sections 2.7 and 3.6 - 3.9).	Functionally define “D3 Assessment” to allow equally valid approaches to meet the same functional objective. Determine whether defensive design measures and pre-planned actions (or coping) fall under the D3 Assessment definition. If not, define those terms as well to ensure that there is a common understanding.
18. 3 “D3 Assessment”	“e. For each postulated accident in the design basis occurring in conjunction with each single postulated CCF, the plant response calculated using realistic or conservative assumptions does not result in radiation release exceeding the applicable siting dose guideline values, violation of the integrity of the primary coolant pressure boundary, or violation of the integrity of the containment (i.e., exceeding coolant system or containment design limits).” This acceptance criterion is a good spot to add guidance on leak-before-break credit and associated operator actions.	Add, "Coping justification may be based upon the availability of systems outside of the scope of the analysis that act to prevent or mitigate the event of concern. For example, CCF coping affecting the response to large-break loss-of-coolant accidents and main steam line breaks have been accepted in the past. 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."

Affected Section	Comment/Basis	Recommendation
19. 3.1 "Means to Eliminate Further Consideration of CCF"	"Many system design and testing attributes, procedures, measures, and practices can contribute to significantly reducing the likelihood of CCF. However, there are certain design attributes that are sufficient to eliminate further consideration of software-based or software logic-based CCF. These attributes include internal diversity and testability. If the licensee or applicant demonstrates that these design attributes of proposed DI&C systems or components meet appropriate criteria, then a CCF-induced malfunction analysis does not need to be performed for those proposed systems or components. Criteria for demonstrating that each of these design attributes are sufficient areprovided in Sections B.3.1.1 and B.3.1.2 below." Use the suggested wording in the Recommendation block.	Changes paragraph to read "Many system design and testing attributes, procedures, measures, and practices can contribute to significantly reducing the likelihood of CCF. However, there are certain design attributes that are sufficient to eliminate further consideration of software-based or software logic-based CCF. These attributes include diversity within the design, comprehensive testing, and design attributes preventing CCFs. If the licensee or applicant demonstrates that these design attributes of proposed DI&C systems or components meet appropriate criteria, then a CCF coping analysis does not need to be performed for those proposed systems or components. Criteria for demonstrating that each of these design attributes are sufficient are provided in Sections B.3.1.1 and B.3.1.2 below."
20. 3.1.1 "Use of Internal Diversity to Eliminate Further Consideration of CCF"	"If this can be demonstrated, no additional diversity would be necessary in the safety system." Use the suggested wording in the Recommendation block.	Change sentence to read "If this can be demonstrated, then it can be concluded that the system is sufficiently protected against CCF vulnerabilities"
21. 3.1.1 "Use of Internal Diversity to Eliminate Further Consideration of CCF"	"To reach a conclusion that no additional diversity is needed for the proposed design, the following criteria should be met:" Use the suggested wording in the Recommendation block.	"To reach a conclusion that sufficient diversity exists for the proposed design, the following criteria should be met:"

Affected Section	Comment/Basis	Recommendation
22. 3.1.1 "Use of Internal Diversity to Eliminate Further Consideration of CCF"	"Each different technology used to perform the credited safety functions is shown to be highly reliable and continually available for the plant conditions during which the associated event is expected to be prevented or mitigated." This is a requirement for a safety system in general and is not specific to internal diversity. "Periodic surveillance criteria are used to verify the continued operability of each channel." The design documents the periodic surveillance, calibration, self-tests, and diagnostics in the replacement system, and the modifications made to the periodic surveillance and calibration required for the existing system. The rationale for those modifications is documented. The documentation demonstrates that the system verifies the continued operability of each channel and the system.	Delete the 3.1.1.c and 3.1.1.d

23. 3.1.2 “Use of Testing to Eliminate Further Consideration of CCF”	3.1.2.a thru 3.1.2.d criteria: The criteria should allow for the possibility of white box testing (i.e. inspecting the software while it is being tested and taking credit for highly controlled internally segmented unoptimized software functions.) Need to simplify the criteria to eliminate the repetition between the criteria and the acceptance criteria. If retained, then clarify: Item b: "all possible timing sequences" needs to be more definitive because it is not clear what time scales (picoseconds, seconds, weeks, months, etc.) and sequences are to be considered. Item c: "some past condition" and "all possible past conditions" is unclear. Item d: It is not clear how we are to demonstrate that unused logic and circuits do not interfere, whether analog or digital, or relays. The flexibility in testability should also recognize the differences in technology between microprocessors and FPGAs. The safety-critical FPGA community is continuing to develop new and different ways to test FPGA-based systems. Some examples include: Assertion Based Verification Constrained Random Verification Universal Verification Methodology Formal Verification Model Based Design	Clarify the testing criteria and acceptance criteria.

Affected Section	Comment/Basis	Recommendation
	The review guidance should acknowledge that other testing alternatives can be proposed and justified.	
24. 3.2.1 "Crediting Existing Systems"	"The function performed by this high reliability I&C system should result in plant consequences that do not exceed the limits prescribed for each AOO or postulated accident in the final safety analysis report." The statement should be revised to link the acceptance criteria described in B.3 above and <u>not</u> the safety analyses. Instead of AOO it should be each DBE.	The acceptance criteria should be linked to Section B.3 and AOO should be changed to DBE.
25. 3.2.1 "Crediting Existing Systems"	3.2.1.c "For both these options, the capabilities for sensing and responding have been shown to meet the response time requirements of the proposed DI&C system for each AOO or postulated accident in SAR." Response time limits are only defined for credited trip signals for Chapter 15 events. They are not defined for diverse actuation systems based on best estimate methodology analyses.	Be specific on which response times are needed for each situation (i.e., AOO or postulated accident).
26. 5 "Spurious Operation"	Regarding all of Section 5: It is not clear what the regulatory requirement is to perform an analysis of potential spurious operations caused by a CCF event.	State the regulatory requirement(s) that would require a licensee to analyze spurious operations caused by a CCF event. Once the licensing basis requirements are sufficiently articulated then it should be easier to identify an appropriate scope of analyses for Section 5.

Affected Section	Comment/Basis	Recommendation
27. 6 “Manual System Level Actuation and Indications”	“Once system-level manual actuation from the MCR using the Position 4 displays and controls has been completed, controls outside the MCR for long-term management of these critical safety functions may be used when supported by suitable HFE analysis and site-specific procedures or instructions.” These requirements should be bounded by the statements of consideration for 10 CFR Part 50, Appendix R. The Position 4 displays and controls should be limited to given the design basis for the particular operating plant.	The section needs to be clarified to ensure that the appropriate scope is established.
28. 6 “Manual System Level Actuation and Indications”	“a. The displays and controls should be sufficient for the operator to monitor and control the following critical safety functions: reactivity level, core heat removal, reactor coolant inventory, containment isolation, and containment integrity.” What if it's just one control to address one DBE that is outside the control room?	The section needs to be clarified to ensure that the appropriate scope is established.