BTP 7-19 Revision 8 Draft - Key Comments from Nuclear Automation Engineering

The following individual comments are submitted from Nuclear Automation Engineering, LLC (NAE) for Docket ID NRC-2019-0253:

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 non-compliant 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.

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.

3. This 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.

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.

5. Section 5.2.b.3.ii goes on to say “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.

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 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.

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."

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.