Comments from Nuclear Automation Engineering on BTP 7-19 - Draft Version for Use at the ACRS Digital Instrumentation and Control Subcommittee Meeting on June 2, 2020

Comments pertaining to guidance that is insufficient to ensure adequate safety. In some cases as noted, this guidance is also inconsistent with previous staff guidance.

1. Failures to be considered as Beyond Design Basis CCF include the following:
   • CCFs resulting from latent hardware or software defects leading to….

   The Commission … indicated that events associated with the triggering of CCF vulnerabilities due to software defects of a DI&C system are considered beyond DBE…

   … while the NRC considers CCF vulnerabilities due to software and hardware defects in DI&C systems to be beyond design basis failures…

   … CCF caused by latent defects …events associated with this type of CCF vulnerability are considered beyond DBE, in accordance with Commission direction in SRM to SECY 93-087

   Comment: The SRM to SECY 93-087 defined CCF due to a design defect as a beyond DBE for safety systems; this was primarily because safety systems have a robust design process, making the likelihood of a design defect very low. This BTP needs to clarify that CCFs due to a design defect are beyond DBEs only for systems developed with a robust design process; this is typically referred to as augmented quality. For systems that are not developed with augmented quality, a CCF due to a design defect should be considered a DBE.

2. These principles provide a framework for addressing CCF vulnerabilities in DI&C systems using a graded approach…

   Vulnerabilities to CCF have been adequately identified and documented, and then the consequences addressed for DI&C systems using a graded approach.

   The guiding principles within SECY-18-0090 clarify that it is acceptable to use a graded approach … to address CCFs.

   This BTP provides a suggested framework for a possible graded approach … to address CCF for the proposed DI&C system.

   Table 2-1: … Implementing a Graded Approach to … Potential CCFs

   Comment: This document also addresses CCF due to single failures; therefore, it is important to clarify that a graded approach is applicable to CCF due to a design defect, but not applicable to CCF due to a single failure. Single failures are within the design basis, because they are expected during the life of the plant. Therefore, they require deterministic analyses the same as any AOO.

3. The results of a qualitative assessment of the vulnerability to CCF for proposed DI&C systems of lower safety significance…

   …the qualitative assessment … is an acceptable method to address potential CCFs in A2, B1, and applicable B2 systems.

   …best-estimate analyses that demonstrate how failure effects are bounded

   The assessment includes thermal-hydraulic analyses using realistic assumptions…

Comment: This document also addresses CCF due to single failures; therefore, it is important to clarify that a qualitative assessment, best estimate methods and realistic assumptions are not applicable to a CCF due to single failures for systems in any safety category. Single failures are within the design basis, because they are expected during the life of the plant. Therefore, they require conservative deterministic analyses the same as any AOO.

4. Vulnerabilities can be prevented or eliminated from further consideration using any of the methods described below…

   …design measures can be used to eliminate or reduce the likelihood of the CCF…

   Comment: Clarify that these methods apply only to CCFs due to a design defect. They do not apply to a CCF due to a random hardware failure, because random hardware failures must be assumed to occur during the life of the plant. Their likelihood cannot be reduced to require no further consideration.

5. Diversity can be implemented by using different technologies, algorithms or logics, sensing devices, or actuation devices.

   Comment: It's technically incorrect to imply that diversity in algorithms or logics, sensing devices, or actuation devices could preclude the need for further consideration of a defect in the digital platform itself; this was the conclusion of NUREG-7007. If the Staff believes there is some level of diversity in algorithms or logics, sensing devices, or actuation devices that can preclude the need for further consideration of a CCF in the digital platform, an example should be provided.

   This section should explain that diversity in elements such as algorithms, I/O and data communication configuration, can be credited to achieve non-concurrent triggers, which is very useful in limiting a CCF that causes spurious operations. But unless the failure from those triggers is self-announcing, as it is for spurious operations, the failure can remain hidden (i.e., a trigger that results in failure-to-actuate remains hidden). Therefore, the hidden trigger can also occur in other redundancies, resulting in a failure-to-actuate CCF in multiple redundancies that must be considered concurrent with AOOs and PAs.

6. …testable based on the following criteria … for PDDs that include analog inputs, the testing of every combination of inputs include the entire operational range of the analog inputs…

   Comment: For an analog input, there are an infinite number of test points over the entire operational range. In addition, there are an infinite number of positive and negative transitions from any steady-state condition. While less than an infinite number of test cases can support a qualitative assessment for categories A2 and B1, less than an infinite number of test cases cannot support a deterministic assessment for category A1.

7. Any manual operator action(s) credited in the D3 assessment can be implemented with sufficient time available for the operators to determine the need for manual operator action…

   Comment: This conflicts with SRP Chapter 18. Time available to determine "the need for manual action" is not sufficient; there must be sufficient margin between the time available and time required to actually execute that action.

8. The equipment used to support manual operator action is … diverse from the automatic safety system…

Comment: Diversity is also required from the manual actions that are normally credited for mitigating some events, such as SGTR, if those manual actions are subject to a CCF due to a design defect; this would be the case in modern highly integrated digital systems.

9. If the proposed system and the new diverse system share resources (e.g. priority modules), the application should demonstrate that the proposed system has priority over the resources when it is operable and available.

   Comment: This is technically incorrect and not consistent with ISG-04. If the primary safety system has priority over the backup diverse system, then a hidden CCF in the primary system, which cannot be determined through operability or availability, can prevent the diverse system from performing its backup safety function. Therefore, there must be safe-state priority, not system priority, as described in ISG-04.

10. Therefore, with regard to spurious operation, the primary concern is … a common latent defect.

    Comment: Technically this statement is not correct. The primary concern is not spurious operation due to a design defect; this is a very rare beyond DBE. The primary concern is a spurious operation due to a single malfunction, because a single malfunction is expected during the life of the plant; therefore, it is a DBE and the plant level results must be bounded by other AOOs or a new AOO must be added to the plant's accident analysis.

11. A block is a physical subset of equipment and software for which it can be credibly assumed that internal failures, including the effects of software and logic errors, will not propagate to other equipment or software.

    Comment: When assessing a defect that results in failure-to-actuate it is reasonable to assume that the output of a block will not propagate to other blocks. But when assessing a defect that results in spurious operation you must follow the signal path to all other blocks that utilize that erroneous output. Therefore, assuming no propagation is not applicable to spurious operations.

12. …a design or implementation defect in this type of block can result in a CCF of all application functions that use that block.

    Comment: As commented in item 26 below, implementation defects should be excluded from this BTP. However, in this sentence “implementation defect” should be replaced by single malfunction, and it should be emphasized that a single malfunction that adversely affects multiple application functions is a DBE that is likely to have unbounded consequences, if a failure of those application functions is analyzed individually in the plant’s accident analyses.

13. …licensees or applicants may potentially credit the ability of plant operators to identify system leakage…

    Comment: Clarify that the leak detection system, and the I&C equipment for operator actions taken in response to leak detection, must:
    a) Be diverse and functionally independent from the CCF in the protection system.
    b) Have augmented quality or be in continuous operation (applies to both detection and mitigation controls).
    c) Must be managed to ensure operability (e.g., Tech Specs or maintenance rule)

Comments pertaining to guidance that imposes an unnecessary burden on the industry without a commensurate safety benefit. In most cases, as noted, this guidance is not consistent with prior regulatory guidance or is not technically correct.

14. Failures required to be addressed within the Design Basis include the following:
    - effects of faults propagated through system interconnectivity
    - effects of faults resulting from failures occurring within shared resources

    Since such failures are likely to occur during the life of the plant…

    Comment: These are only correct if those faults are due to single malfunctions, not design defects. This BTP must clearly distinguish these two different sources of CCF.

15. RG 1.53, "Application of the Single-Failure Criterion to Safety Systems," provides guidance…

    Spurious Operations required to be addressed as part of the design basis include: Spurious operations as a result of single failures…

    Comment: The single failure criterion (SFC) has never been applied to prevention of spurious operations. This is because the SFC includes consideration of electrical faults, failure of passive components (e.g., wires and terminations), fire and flood. For the evaluation of spurious operations only single failures in active components should be considered; these have been distinguished from single failures using the term 'single malfunctions'. This BTP needs to distinguish single malfunctions from single failures.

16. Beyond Design Basis failures, the subject of this document… If such a possible CCF cannot be prevented… consequences must remain acceptable within the plant design basis limits.

    The D3 assessment … ensure that the consequences of the CCF are bounded within the limits deemed to be acceptable per the plant safety analysis.

    The consequences of any residual CCF vulnerabilities … must be … acceptable within the plant design basis.

    …how the residual risk has been bounded within the allowable limits of the safety analysis

    … verifying that plant conditions stay within the acceptance criteria specified for each AOO or PA in the SAR.

    A new diverse system…the functions performed by this diverse means are adequate to maintain plant conditions within specified acceptance criteria for the associated DBE…

    …the application demonstrates that the following acceptance criteria are met…The functions performed by the diverse system are adequate to maintain plant conditions within the specified acceptance criteria for the associated DBEs

    …best-estimate analyses may be performed to show that the potential consequences of postulated failures are bounded

    Comment: These paragraphs are referring to a CCF due to a design defect, which are beyond design basis events. Therefore, the consequences do not have to remain within the limits for design basis events. Beyond design basis acceptance criteria should be defined to maintain coolant boundary integrity, containment integrity, and core coolability or 10CFR100 offsite dose limits. This is especially important for spurious operations.

17. This document provides guidance for … latent defects. Section B.2 of this BTP identifies an example of a general framework for a graded approach ....

    Comment: This document also addresses CCF due to single failures; therefore, it is important to clarify that a graded approach is not applicable to CCF due to single failures. Single failures are within the design basis, because they are expected during the life of the plant. Therefore, they require deterministic analyses the same as any AOO.

18. The monitoring and indicator system echelon consists of …independent manual controls … independent of the three other echelons of defense, such that no monitoring or system-level actuation equipment … is vulnerable to failure due to a cause that is common to that of one or more of the other echelons.

    All of these systems are backed up by plant operators using the monitoring and indicator system to independently acquire the data ....

    Comment: Independence between automation and monitoring/controls within the plant safety system are not require by any regulation, including IEEE-603. Requiring this independence adds unnecessary cost to the design of plant safety systems. This BTP ensures that backup monitoring and control is provided to accommodate a CCF that adversely affects both automation and manual control within the plant safety system. That is sufficient.

19. …the triggering of CCF vulnerabilities … the evaluation of such events should use best-estimate methods.

    Comment: There is no requirement to evaluate the events that trigger CCFs, because we don't know what events trigger CCFs. Since CCFs that result in failure-to-actuate remain hidden, the requirement from the SRM to SECY 93-087 is to evaluate AOOs and PAs concurrent with a CCF in the plant safety system, not to evaluate the event that triggered the CCF.

20. This BTP also addresses the applicant’s assessment of vulnerabilities to a CCF due to latent software or hardware defects that can cause the spurious operation… such conditions must be included within the design basis and addressed in the plant safety analysis.

    Comment: A CCF due to a design defect in a system with a robust design process is not within the design basis and is not required to be addressed in the plant safety analysis. Design basis CCFs are those caused by a single failure, or caused by a design defect in a system not designed with a robust design process.

21. The term “best estimate methods” … are defined as the initial plant conditions…

    Comment: Best-estimate methods also relax the acceptance criteria for the event analysis results.

22. …if the initiating event is the loss of offsite power, the assessment does not need to assume another concurrent DBE.

    Comment: This does not clarify that if the event is not initiated by loss of offsite power (e.g. a large pipe break) then loss of offsite power does not need to be considered concurrent with that event, as it is in the DBE accident analysis. The technical basis is that a loss of offsite power is a CCF of two grid connections to two offsite power sources; two unrelated CCFs (i.e., digital and power) are sufficiently unlikely to not require further consideration.

23. The diverse means may be equipment that is NSR with a documented basis that the diverse means is of sufficient quality…

    If the equipment used to perform the credited manual operator action is NSR, then … demonstrate that the equipment used is highly reliable and of adequate quality....

    Comment: The Staff has not required demonstration of sufficient quality for systems that are in continuous operation (e.g., main feedwater control system), because their failure is immediately self-announcing and correctable. In addition, for manual actions if it can be demonstrated that the manual indications and controls are used frequently, then failures are also self-announcing and there should be no requirement to demonstrate augmented quality.

24. Position 4 directs the inclusion of a set of displays and manual controls (“safety” or “non-safety”) in the main control room (MCR) that is independent and diverse from any vulnerability to a CCF…

    The same … analog technology should not be used for both mitigating the DBE and providing signals to these displays and controls to meet Position 4.

    The displays and controls used to address Position 4 shall be independent and diverse from the safety-related DI&C systems that are vulnerable to a CCF…

    The displays and controls are independent … from the safety-related DI&C systems…

    …controls and displays…are independent … from the proposed system…

    Comment: "Independent" implies electrical independence in accordance with RG 1.75. But there is no requirement for this independence for any backup automation or backup manual control. The only requirement is that the backup not be affected by a digital design defect that affects the primary system. Therefore, clarify that independence refers to functional independence from the CCF, not electrical independence. Also, correct that the same analog technology may be used for both mitigating the DBE and Position, because analog technology cannot have a digital design defect.

25. This includes CCFs … caused by spurious operation …To address these potential CCFs, the NRC staff should verify that for each event analyzed in the accident analysis section of the SAR…

    … for each event analyzed in the accident analysis section of the SAR, the results of the D3 assessment indicates that vulnerabilities to CCF have been adequately addressed.

    Spurious operations …must be evaluated in a manner consistent with SRM to SECY 93-087.

    Comment: Clarify that concurrent AOOs/PAs do not require consideration with spurious operations due to either a single failure or a design defect, because spurious operations are self-announcing and can be corrected prior to other plant events.

26. …identified vulnerabilities to CCFs due to a … implementation defect…

    …certain design attributes are sufficient to eliminate from further consideration a potential CCF due to a … implementation defect.

…CCF as a result of errors or defects introduced during the implementation or fabrication of the software, hardware…

…latent defects introduced during the … implementation process

Testing can be used to uncover latent defects … in the … fabrication, and implementation process…

To credit testing as a means of demonstrating that potential … fabrication, and implementation errors have been identified…

Spurious Operations are beyond design basis if they result from … latent hardware defects…

…a[n]... implementation defect in this type of block can result in a CCF of all application functions that use that block.

Comment: There is no regulatory basis for including CCFs due to implementation or fabrication defects in this BTP. Implementation and fabrication defects are precluded by quality assurance programs for manufacturing. If you introduce implementation defects as a potential source of CCF, then to preclude a defect using testing, even for simple devices, would require exhaustive testing for every fabricated component. All instances of “defect” should be changed to “design defect”.

27. A1 DI&C SSCs… should include a D3 assessment …

    …the qualitative assessment … is an acceptable method to address potential CCFs in A2, B1, and applicable B2 systems.

    Spurious Operation Assessment…address the CCF vulnerability through a qualitative assessment for A2, B1 or B2 systems…

    Potential spurious operations due to a CCF vulnerability in an A1 system have been addressed through use of design attributes, defensive measures or diverse means to prevent, limit, or mitigate the consequence of a CCF.

    Comment: This BTP addresses design defects that lead to failure-to-actuate and spurious operations. Spurious operation of B1 systems are typically more risk significant than spurious operations of A1 systems, because they present more severe challenges to critical safety functions (e.g., overpressure, overcooling, damage to pump seals). Since a qualitative assessment is permitted to assess spurious operations for B1 systems, it should also be permitted for the evaluation of a spurious operations due to a design defect in A1 systems; a D3 assessment should not be required for any spurious operations.

28. B2 DI&C SSCs… An analysis demonstrates…

    Comment: The grading classification process already concluded that systems in this category have no direct impact on critical safety functions. Therefore, these systems require no additional analysis and no "qualitative assessment".

29. Once potential sources of CCF have been identified, and feasible design features for preventing, limiting, mitigating, or coping measures have been incorporated to address them, licensees and applicants need to reassess the effects of any remaining (residual) risk…

    …an assessment of the consequences of any residual risks from CCFs…

Comment: The D3 assessment is a deterministic analysis. These paragraphs impose an additional risk assessment that is not required by regulation or the SRM to SECY 93-087 and adds no value. CCF risks are already assessed in the PRA.

30. … such that no further evaluation is necessary … Thus, separate diverse means do not need to be provided, and an analysis of the plant's response for each AOO or postulated accident concurrent with a CCF of the proposed system does not need to be performed…

    Comment: The following should be added - In addition, spurious operations that might otherwise have been caused by a potential design defect do not need to be evaluated.

31. However, diversity needs to be paired with independence otherwise the diverse means could be susceptible to the same vulnerability.

    Each safety function … is shown to be independently achievable by each diverse portion in the system.

    Diversity … is deemed adequate if the safety function can be accomplished independently by each set of diverse equipment …

    … supported by instrumentation independent from the safety system…

    The equipment used to support manual operator action is independent … from the automatic safety system…

    Comment: "Independence", "independent" and "independently" imply electrical independence in accordance with RG 1.75. But there is no requirement for independence between diverse elements within the same division. The only requirement is that each diverse element not be adversely affected by a design defect that adversely affects the other diverse element. Therefore, clarify that independence refers to functional independence from the design defect, not electrical independence.

32. Each diverse portion … is shown to be … continually available…

    Comment: "Continually available" implies that no out-of-service time would be acceptable, even if that time is controlled by TS LCOs. This would mean that each diverse element must also have redundancy. Change to: If diversity is credited within a division or among divisions, then Technical Specification Limiting Condition of Operation Completion Times and Bypass Times reflect the additional dependence on that diversity for preventing CCF.

33. The ATWS system to be credited should (1) be diverse from the proposed DI&C system… and (3) be responsive to the AOO or PA sequences using independent sensors and actuators as the proposed DI&C system.

    Comment: Diverse sensors are not required for compliance to 10CFR50.62. Diverse reactor trip actuators are required only for some plant designs (e.g., CE plants). No other specifically diverse actuators are required for compliance to 10CFR50.62, because ESF actuators (e.g., auxiliary feedwater) are inherently diverse from RT actuators. For this BTP, which extends beyond ATWS events, to preclude a CCF due to a digital design defect in sensors/actuators, diversity should be required, but only if sensors/actuators are digital. Independence is not required for compliance to 10CFR50.62 and should not be required for this BTP. For this BTP, the primary and backup systems can share the same sensors and actuators, as long as they are not a source of CCF due to a design defect (i.e., if they are not digital or a digital design defect has been shown to require no further consideration).

34. …the application shows that the following acceptance criteria are met… For each AOO … occurring in conjunction with the CCF… does not result in radiation release exceeding 10 percent of the applicable siting dose guideline values …

    Comment: Since the SRM to SECY 93-087 defines a CCF due to a design defect in a system with a robust design process as a beyond DBE, there is no regulatory basis to have different acceptance criteria for AOOs vs. PAs. Even when risk is considered, the extremely low likelihood of a CCF makes the risk difference between an AOO with CCF and PA with CCF irrelevant. Therefore, the acceptance criteria for PAs (item b) should be used for all events. Using the PA acceptance criteria for all events will reduce the analysis effort, because the acceptance criteria can be demonstrated for most events using qualitative methods, rather than calculations using safety analysis models and codes. The additional cost for requiring calculations for more events provides an unwarranted safety benefit.

35. … the reviewer should reach a conclusion that the accident analysis results have not been invalidated due to potential spurious operations …

    … the consequences resulting from spurious operation of safety-related or non-safety related components are bounded by the events analyzed in the accident analysis…If not bounded, they are identified as new AOOs…

    …the proposed design will not introduce any conditions that are unbounded by the events in the accident analysis…

    The consequence of a potential spurious operation due to a CCF is bounded

    Comment: These statements are correct for spurious operations cause by a single malfunction (i.e., the plant level result must be bounded by the current accident analysis or as stated, the accident analysis results have not been invalidated). However, spurious operations caused by a design defect in a system with a robust design process are beyond DBEs; therefore, the acceptance criteria should be the same as for other beyond DBEs (i.e., maintain RCS integrity and containment integrity, maintain fuel integrity or offsite dose limits). The acceptance criteria for a CCF due to a single malfunction vs. a design defect need to be distinguished.

36. The reviewer should reach a conclusion that the manual controls and supporting indications conform to Position 4…Section 3.2.2 of this BTP presents the acceptance criteria. The application should sufficiently demonstrate … that the plant remains within analyzed limits.

    Comment: While some Position 4 controls may be credited for mitigating a specific event for Position 3, in general Position 4 is not intended for any specific event mitigation. Position 4 controls are intended for the events we did not anticipate. Therefore, for Position 4 compliance, there should be no additional analysis and no event-based acceptance criteria. Any analysis and demonstration of acceptance criteria should be limited to Position 3. The acceptance criteria for Position 4 should be only that plant systems can be actuated which are expected to control the critical safety functions and that the critical safety functions can be monitored.

37. …Position 4 … single failures concurrent with a CCF do not need to be postulated and normal alignment of equipment is assumed, the capability for manual actuation of a single division is sufficient.

    Comment: This same statement regarding single failure and normal alignment is applicable to all backup functions (i.e., automatic and manual), not just Position 4.

38. Justification should be provided …This includes previously NRC-approved credited manual operator actions in the licensing basis to address AOOs or PAs.

    Comment: The Staff has no regulatory basis to re-review previously approved manual actions, unless those manual actions are being credited for a different purpose, or utilize different indications and controls.