As of: 3/30/18 6:14 AM
Received: March 29, 2018
Status: Pending_Post
Tracking No. 1k2-92ac-3ifc
Comments Due: March 29, 2018
Submission Type: Web

PUBLIC SUBMISSION

Docket: NRC-2018-0044
Clarification on Endorsement of Nuclear Energy Institute Guidance in Designing Digital Upgrades in Instrumentation and Control Systems

Comment On: NRC-2018-0044-0001
Clarification on Endorsement of Nuclear Energy Institute Guidance in Designing Digital Upgrades in Instrumentation and Control Systems

Document: NRC-2018-0044-DRAFT-0006
Comment on FR Doc # 2018-04958

Submitter Information

Name: Ken Scarola
Address:
3672 PINE TREE LN
MURRYSVILLE, 15668
Email: KenScarola@NuclearAutomation.com

General Comment

Please find attached my comments on draft Regulatory Issue Summary (RIS) 2002-22, Supplement 1, "Clarification on Endorsement of Nuclear Energy Institute Guidance in Designing Digital Upgrades in Instrumentation and Control Systems", Docket ID NRC-2018-0044.

Thank you for the opportunity to comment on this very important document.

Ken

Attachments

83 FR 11154
3/14/2018 (6)

2018-03-28 NAE Comments on Draft RIS provided for Public Comment

SUNSI Review Complete
Template = ADM – 013
E-RIDS= ADM-03
Add= Tekia Govan (TXG1)

Comments on DRAFT NRC REGULATORY ISSUE SUMMARY 2002-22, SUPPLEMENT 1
ML18051A084, Docket ID NRC-2018-0044 – Ken Scarola, Nuclear Automation Engineering

General Comment
There should be no question that digital technology offers the inherent capabilities of integration, interconnectivity, and standardization that can reduce nuclear power O&M costs, and improve plant performance and availability, while maintaining or even improving plant safety. For this reason, I have (for more than 40 years) and will continue to be one of the strongest industry advocates for the digital transition.

However, there should also be no question that, if not correctly designed, these same inherent capabilities for integration, interconnectivity and standardization have the potential to create unanalyzed malfunctions that may not be bounded by previous plant analyses; thereby, creating unanalyzed plant conditions that may challenge the 50.59 criteria, and even worse may threaten plant safety.

We can rely on subjective assessments of design processes and/or operating experience to consciously gloss over this potential, as currently written in this RIS, or we can maintain the defense-in-depth foundation of the nuclear power industry by ensuring:

(1) That deterministic design attributes are needed to reach a conclusion that the malfunction likelihood is "sufficiently low" and therefore the effects of failure do not need to be considered in the 50.59 evaluation, with those deterministic attributes being commensurate with the consequences of a postulated failure (i.e., more conservative for safety functions).

AND

(2) For digital upgrades that cannot reach the "sufficiently low" likelihood threshold, we can establish reasonable processes for evaluating potential new malfunctions, commensurate with their malfunction likelihood, to ensure these new malfunctions are bounded by previous analyses.

If the RIS is clear on these two technical points, then digital upgrades under 50.59 will be unquestionably safe, and therefore will not need Staff review/approval. If the RIS is not clear on the requirement for deterministic attributes, then the NRC will be giving licensees the authority to make qualitative judgements that only NRC should be making, because non-conservatism in these subjective judgements will adversely affect plant safety.

All comments below are an extension of this one key message.

Specific Comments

1. The purpose for the distinction between Qualitative Assessments in Section 3 and Engineering Evaluations in Section 4 is not clear. Both sections overlap considerably (~8 pages); this unnecessarily complicates the RIS. This licensing vs. engineering distinction does not exist in prior regulatory criteria. Instead of a cohesive NRC position, this distinction reflects internal differences within NRC and therefore, will continue to foster the industry's fear that there is too much licensing uncertainty to proceed with digital upgrades.

   If this distinction is needed for some internal NRC reason (that I don't understand), then Engineering Evaluations, that are conducted under the appropriate NRC approved quality assurance program (QAP) for the equipment being replaced, should be described first, because these evaluations should be clearly identified as perquisites to the Qualitative Assessments. Then the Qualitative Assessment should explain how the Engineering Evaluation output is used to arrive at the Qualitative Assessment. As written now, there is no discussion of input from the Engineering Evaluation in the Qualitative Assessment. The Qualitative Assessment is not an independent task; the RIS must be clear that a necessary component of the Qualitative Assessment is an Engineering Evaluation with appropriate quality assurance.

The RIS should also be clear on what is the necessary and sufficient content of that Engineering Evaluation to avoid a violation. Specific criteria are need for the engineers to know what must be done. Without this clarity, the RIS will underscore industry's fear of regulatory uncertainty that will continue to deter digital upgrades.

An alternative that I prefer, is to completely delete Section 4 and simply ensure that the engineering evaluations that are needed to document the Qualitative Assessments are clearly explained in Section 3 (with clear minimum content requirements, including the need for deterministic design attributes to reach a "sufficiently low" conclusion, see Comment 6), along with clarification that, since these Qualitative Assessments include engineering evaluations, these Qualitative Assessments are performed under the appropriate QAP for the equipment being replaced. This would better reflect the actual industry practice, where Qualitative Assessments are most often conducted as part of the engineering process.

2. The RIS gives licensees the discretion to determine what design attributes can be credited (if any are needed at all, see Comment 6) to reach a Qualitative Assessment conclusion that the likelihood of failure is "sufficiently low". As written (page 2 paragraph 2), this licensee discretion is applicable to all digital upgrades, except RTS and ESFAS, which are excluded from the scope of this RIS. Applying this discretion to other systems that are not RTS or ESFAS, but are within the scope of BTP 7-19 Revision 6 (i.e., "ESF auxiliary supporting features... a safety function that is credited in the safety analysis to respond to the DBE") and the SRM to SECY 93-087 (i.e., "a safety function") creates a conflict with BTP 7-19, because BTP 7-19 is applicable to "both the currently operating NPPs licensed under 10 CFR Part 50 and new NPPs licensed under 10 CFR Part 52". Giving licensees discretion to determine acceptable design attributes conflicts with BTP 7-19, because BTP 7-19 defines only two design attributes that can be credited to reach a "sufficiently low" conclusion – (1) simplicity (as demonstrated through 100% testability) or (2) internal diversity; BTP 7-19 refers to this as "sufficient to eliminate consideration of software based or software logic based CCF", which is equivalent to the RIS definition of "sufficiently low".

   In ML13298A787 NRC noted the concern that the criteria in NEI 01-01 Section 4.1.2 for "acceptably low", which is equivalent to the RIS definition of "sufficiently low", are "less conservative that those ...in BTP 7-19".

   I can suggest two alternatives for resolving this conflict:

   a) In addition to RTS and ESFAS, exclude from the scope of the RIS 'ESF auxiliary supporting features and other safety functions that are credited in responding to DBEs'. The RIS is currently ambiguous on this issue. The first paragraph on Page 2, excludes only reactor protection systems and engineered safety features actuation systems from the RIS. But Page 5, item 1.c implies that ESF control logic and load sequencers are also excluded.

   OR

   b) Clarify that for 'ESF auxiliary supporting features and other safety functions that are credited in responding to DBEs", design attributes of (1) simplicity (as demonstrated through 100% testability) or (2) internal diversity, are needed to reach the "sufficiently low" threshold. For simplicity, the RIS should provide guidance for the Qualitative Assessments to address the relevance of untested sequences; this guidance should be consistent with the Staff's Final Safety Evaluation Report for the Westinghouse SSPS Board Replacement, ML14260A143.

   My preference is for alternative (b), because digital upgrades are needed for these ESF functions.

   Either alternative recognizes that many ESF auxiliary features, such as emergency load sequencers, displays (i.e., for RG 1.97 Type A variables) and controls that support manual actions that are credited in the transient and accident analysis, and SSCs that support both manual and automatic

ESF actions, are at least as safety significant, and in some cases even more safety significant, than RTS and ESFAS.

Alternative (b) would result in more conservative criteria to reach the "sufficiently low" threshold, for safety equipment compared to non-safety equipment. This additional conservatism is consistent with all prior NRC guidance for safety and non-safety systems. More conservative criteria are appropriate due to the more significant consequences of safety equipment failure.

Please note that changing the criteria, through this RIS, for precluding the need to consider a CCF for these safety significant design functions, creates an inconsistency between the regulatory criteria for new plants and operating plants. This is not only contrary to the SRM to SECY 93-087 and BTP 7-19, but also contrary to the Commissioners' direction in their response to SECY-15-0106 where they state "the same requirements should apply to operating and new reactors". If you continue down this path, the RIS development schedule should identify when you will inform the Commissioners that the Staff is proceeding contrary to their direction for "an integrated strategy to modernize the NRC's digital instrumentation and control (I&C) regulatory infrastructure."

In conjunction with either resolution above, industry and NRC should expedite efforts to reach agreement on other design attributes that can be credited to reach a "sufficiently low" conclusion for all safety significant SSCs (i.e., simplicity and diversity are not the only ones).

3. NRC and industry have both identified screening as a key source of 50.59 errors and inconsistency throughout the industry. In ML13298A787, NRC specifically identifies that NEI 01-01 Section 4.3.2 provides incorrect screening guidance, which results in no Qualitative Assessments, even for new digital devices applied to redundant safety systems.

   Due to the increased complexity of digital technology compared to analog technology, the potential for a digital design defect is inherently higher than a design defect in the predecessor analog technology; therefore, there is always the potential for a malfunction with a different result. To ensure all digital upgrades receive proper licensing consideration, and thereby resolve this key source of 50.59 errors and inconsistency, the RIS should clarify that all digital upgrades to design functions screen-in. If the RIS remains silent on this issue (Attachment page 1, paragraph 2), there can be no expectation that the previous errors and inconsistencies in screening for digital upgrades will not continue.

4. The RIS incorrectly implies that a "sufficiently low" conclusion is necessary for favorable answers to 50.59 questions i, ii, v and vi (Attachment, section "Likelihood Thresholds for 10 CFR 50.59(c)(2)(i), (ii), (v), and (vi)"). For questions i and ii, a marginal increase in likelihood, compared to the analog predecessor is acceptable (i.e., "sufficiently low" likelihood is not required). For questions v and vi, malfunction likelihood is irrelevant if the malfunction result is not different.

   The RIS should clarify that a "sufficiently low" conclusion is only needed to preclude evaluation of any potential malfunctions when answering questions v and vi. Therefore, if the Qualitative Assessments cannot reach a "sufficiently low" conclusion, that does not mean that the digital upgrade requires an LAR. It only means that a malfunction due to a failure of that digital component must be analyzed when answering 50.59 Questions v and vi.

   In this regard, all discussion of reaching the "sufficiently low" threshold for 50.59 Questions i and ii should be deleted; this will simplify the RIS and reduce licensing confusion.

   Considering the comments above, the RIS should be changed (Attachment, page 2, last paragraph) to identify four potential outcomes of the Qualitative Assessment:

   a) Failure likelihood is "sufficiently low" – a malfunction result evaluation is not needed for 50.59 Questions v and vi. In addition to an assessment of design process and/or operating history, deterministic design attributes are also needed to reach this threshold.

b) Failure likelihood is not "sufficiently low" but is no more than a marginal increase compared to its analog predecessor and not significantly lower than a single random hardware failure – a malfunction result evaluation is needed for 50.59 Questions v and vi using conservative design basis methods.
c) Failure likelihood is not "sufficiently low" but is significantly lower than a single random hardware failure – a malfunction result evaluation is needed for 50.59 Questions v and vi; that evaluation may use less conservative beyond design basis (i.e., "best estimate") methods. Consistent with the guidance in the SRM to SECY 93-087 and BTP 7-19, when there are no shared hardware resources among multiple SSCs, the threshold of 'significantly lower than a single random hardware failure" can be reached with an assessment of design process and/or operating history.
d) Failure likelihood is not "sufficiently low" and is more than a marginal increase compared to its analog predecessor – an LAR is needed based on 50.59 Question ii.

5. The RIS is ambiguous regarding the use of "best-estimate" methods for assessing the malfunction results (Attachment page 12, paragraph 3; Section 2.1, last sentence) when a "sufficiently low" likelihood threshold cannot be achieved. My interpretation of the current draft wording is that for plants whose UFSAR analyses use "best-estimate" methods for beyond design basis events, such as ATWS, SBO or safe shutdown for exposure fires, "best-estimate" methods can also be used to determine the results of digital malfunctions that are considered beyond design basis, when answering 50.59 Questions v and vi.

   I base this interpretation on my assessment of the 10CFR50.59 rule and statements of consideration, neither of which preclude the use of best-estimate methods. In addition, it would be very unusual for the Staff to use a RIS to preclude consideration of beyond design basis malfunctions that the Commission has decreed must be considered through the SRM to SECY 93-087.

   As defined in the SRM to SECY-93-087 and BTP 7-19, this would apply to malfunctions due to a digital design defect in digital applications that have a robust design process, as determined through the Qualitative Assessments, because these malfunctions are significantly less likely than malfunctions due to a single random hardware failure; therefore, they are considered beyond design basis events. The RIS should clarify this point. The Staff may also want to clarify that the SRM to SECY 93-087 limits the use of best-estimate methods to beyond design basis digital malfunctions; therefore, the RIS does not endorse the use of best-estimate methods for other malfunctions.

   However, the RIS should also clarify that malfunctions due to a random failure of a shared hardware resource (i.e., CCFs) are not beyond design basis events. Therefore, unless a "sufficiently low" likelihood threshold can be achieved, the malfunction results must be determined using conservative design basis methods, when answering 50.59 Questions v and vi.

   The RIS should clarify the key differences between conservative and "best-estimate" methods for the analysis of digital malfunctions, and how those differences are applied when analyzing malfunctions for digital initiators vs. digital mitigators (e.g., concurrent events that must be considered, equipment and manual actions that can be credited for mitigation, acceptance criteria). If the Staff is not willing to expand the RIS to provide this additional guidance for digital malfunctions, as a minimum, the RIS should refer to BTP 7-19 for guidance on "best-estimate" analysis methods for beyond design basis digital malfunctions.

   If my interpretation of the current RIS is incorrect, and the RIS does not consider a malfunction due to a design defect to be a beyond design basis event (equivalent to ATWS and other previously analyzed beyond design basis events), and thereby does not permit "best-estimate" methods to be used when determining the malfunction results, digital upgrades will be limited to those where a "sufficiently low" conclusion can be reached. This will preclude digital upgrades to most design functions that operate in a standby mode (i.e., most safety functions credited for responding to DBEs), because even if non-concurrent triggers can be defended, self-announcing cannot; therefore,

non-concurrent triggers can accumulate to become a CCF (i.e., the CCF likelihood is not "sufficiently low").

Not allowing a malfunction due to a design defect in a system with a robust design process to be analyzed as a beyond design basis event, using "best-estimate" methods, would be inconsistent with NEI 01-01, which states "re-analysis of design basis events is permitted using "best estimate" conditions with realistic assumptions, rather than the more conservative design basis conditions required in 10 CFR 50, Appendix K... the results of the analysis feed into the design and licensing process (including the failure analysis)". In addition, Example 5-7 employs the "best-estimate" analysis methods of BTP 7-19 to demonstrate that manual actions can be credited as "part of the overall change in the 50.59 evaluation" when there is a beyond design basis CCF that adversely affects the automated actions. Page 1 of the RIS states "NRC continues to endorse NEI 01-01".

Not allowing a malfunction due to a design defect to be analyzed as a beyond design basis event, using "best-estimate" methods, would also create an inconsistency between the regulatory criteria for new plants and operating plants in the SRM to SECY 93-087 and BTP 7-19. This is contrary to the Commissioners' direction in their response to SECY-15-0106 where they state "the same requirements should apply to operating and new reactors". The current guidance in NEI 01-01 for operating plants is consistent with the guidance in the SRM to SECY 93-087 and BTP 7-19 for new plants. If you continue down this path of creating an inconsistency between the regulatory criteria for new plants and operating plants, the RIS development schedule should identify when you will inform the Commissioners that the Staff is proceeding contrary to their direction for "an integrated strategy to modernize the NRC's digital instrumentation and control (I&C) regulatory infrastructure.".

6. The RIS is ambiguous regarding the need for design attributes to reach a "sufficiently low" conclusion in the Qualitative Assessments. In Sections 3.1 and 4.5, clarify that quality of the design process and/or operating experience, cannot be credited alone to achieve a "sufficiently low" threshold. Design attributes (e.g., simple, diverse, application differences to prevent concurrent triggers) are also needed to reduce the likelihood of a malfunction due to a failure of a shared hardware or design resource, and thereby reach the "sufficiently low" threshold. The RIS must be explicitly clear on what is necessary and sufficient to avoid a violation.

   Currently, Section 3.1 says "nor does the qualitative assessment need to address each specific item"; the implication is that design attributes are not needed to reach a "sufficiently low" threshold.

   Section 4.5 paragraph 2 requires "design features and attributes", but then paragraph 4 confuses this issue by limiting this to "complex modifications". Clarify that simplicity is a design attribute, but where simplicity cannot be demonstrated, then other design attributes (e.g., diversity, application differences to prevent concurrent triggers) are needed.

   In this regard, the RIS should also clarify that some text in NEI 01-01 (e.g., last paragraph on page 4-20) and some examples in NEI 01-01 (e.g., Example 4-8, 5-3) are incorrect, where there is a reliance on only the quality of the design process and/or operating experience to reach a conclusion that a software CCF does not need to be considered as a possible malfunction with a different result. Similarly, Example 5-1 incorrectly states that a software CCF requires no consideration when assessing new potential failure modes. The errors in Examples 5-1, 5-3 were identified by NRC in ML13298A787 (see Comment 7, below).

7. ML13298A787, November 5, 2013 identifies many issues, including errors in NEI 01-01, that have deterred digital upgrades. To avoid continued industry confusion, this RIS needs to address these issues, including those noted within these comments, and state that this RIS resolves the issues raised by NRC in ML13298A787, November 5, 2013 as they pertain to digital equipment within the scope of this RIS. Alternately, this RIS could identify the issues that remain outstanding. By not addressing ML13298A787 at all, continued licensing uncertain will remain a serious deterrent to digital upgrades.

8. The inclusion of "design flaws" in the NEI 01-01 definition of "sufficiently low" as an example of "common cause failures that are not considered in the UFSAR" (RIS page 2, footnote) has been a key source of 50.59 errors and inconsistencies. The RIS needs to clarify that this NEI 01-01 example pertains only to analog design flaws, which were the only design flaws considered in the UFSARs at the time NEI 01-01 was written. Due to the inherent complexity of current digital technology, the potential for a digital design defect is higher than a design defect in the predecessor analog technology; therefore, the likelihood of a digital design defect is not comparable to other common cause failures not considered in the UFSAR.

   Therefore, the RIS also needs to clarify that where a digital design is shared among multiple SSCs (i.e., a digital design is a shared resource), safety or non-safety, a malfunction due to a defect in that digital design must be evaluated for 50.59 Questions v and vi, unless design attributes support a Qualitative Assessment conclusion that the likelihood of a CCF due to that digital design defect is "sufficiently low" (i.e., comparable to calibration errors, maintenance errors, environmental stresses that exceed equipment qualification/testing envelopes).

9. The NRC and industry focus on CCF due to software has led to confusion, because there are complex digital devices such as FPGAs and PLDs that do not contain software. All instances of software in this RIS (e.g., software CCF) should be changed to "digital" or "digital design" (as appropriate for the specific context) unless there is a statement with specific applicability to software only (I don't think there are any). This change would be consistent with RIS 2016-05 Embedded Digital Devices in Safety Related Systems.

10. In Section 3, the RIS explains the potential for new malfunctions when design functions are combined. It needs to also explain the potential for new malfunctions when design functions are interconnected in any manner, digital or hardwired, or when the same digital design is used for multiple design functions (e.g., a common digital platform or device). The RIS should clarify that this concern applies to safety and non-safety systems. Any type of integration (through shared/interconnected hardware or a shared design) creates a CCF vulnerability (Attachment, page 5, item 1(a)); the purpose of the Qualitative Assessments is to demonstrate that the vulnerability is "sufficiently low" so that no further malfunction results analysis is needed for 50.59 Questions v and vi.

    The RIS should clarify that any interconnections can propagate erroneous control data between design functions, causing new functional malfunctions. Even unidirectional digital data communication can result in failure of the transmitting digital device, because most unidirectional data communication includes handshaking, whose errors can disrupt the deterministic processing of the transmitting digital device. One method of precluding handshaking can be by using a fiber optic interface with only a transmission fiber (no receive fiber), but this is uncommon. Disruption to the deterministic processing of one or more digital devices can also occur due to data storms, even when the digital data communication is not used for control.

    When performing the Qualitative Assessments and attempting to reach a "sufficiently low" threshold, specific design attributes, such as the communication independence attributes described in ISG-04, can be applied to prevent a CCF due to interconnections. However, the RIS should be very clear that justification is needed for any non-compliance to ISG-04 for any safety system inter-division communication, since this is the current NRC guidance for safety systems. Alternate methods of maintaining independence for intra-division communication within safety or non-safety systems can be defended without this non-compliance justification.

    The RIS should clarify that when the same digital design is used for multiple design functions, safety or non-safety, that digital design is a shared resource, whose failure can adversely and concurrently affect those design functions (i.e., a CCF). When performing the Qualitative Assessments and attempting to reach a "sufficiently low" threshold, specific design attributes, such as configuration differences to prevent concurrent triggers (with self-announcing), can be applied to prevent a CCF due to a design defect in that shared resource. However, the RIS should be very clear that (until

additional preventive measures are approved by the Staff) only simplicity or internal diversity can be credited to preclude a CCF due to a design defect for any safety functions credited for DBE mitigation (see Comment 2); licensees may credit other preventive measures (e.g., non-concurrent triggers with self-announcing) for other SSCs.

The RIS should clarify (Attachment page 5, Item 2) that a shared digital design reduces independence, unless the CCF likelihood due to a design defect is concluded to be much lower than a CCF due to a single random hardware failure. This is because the likelihood of a digital design defect is higher than its analog predecessor; therefore, a CCF is inherently more likely, unless specific design attributes are included to reduce its likelihood so that the CCF can be treated as a beyond design basis event (as defined in the SRM to SECY-93-087 and BTP 7-19). It is important to note that the likelihood threshold for "much lower than a CCF due to a single random hardware" to be considered beyond design basis, is not as conservative as the "sufficiently low" threshold for which no further malfunction consideration is needed for the CCF (see Comments 4 and 5).

The RIS should clarify that any type of combining, sharing or interconnecting of safety or non-safety design functions that were previously separated, can result in CCFs that may cause unanalyzed transients. These CCFs may only affect non-safety SSCs that are not credited in the UFSAR for accident mitigation, or they may be within the same safety or non-safety echelon of defense (contrary to the statements in Attachment Section 4.2.2); regardless of the source, any potential CCF that can result in an unanalyzed transient is a concern when answering 50.59 questions v and vi.

11. Page 2, paragraph 2 – Change RPS to RTS, because in other regulatory documents RPS encompasses RTS and ESFAS (e.g., BTP 7-19).

12. Attachment, page 3, paragraph 1

    The statement that digital increases the likelihood of failure is not correct; digital equipment is typically much more reliable than its analog predecessor. The concern is that digital is inherently more adaptable to shared resources, including shared interconnections, and shared designs among multiple design functions and multiple SSCs, both of which can lead to different malfunctions.

    The statement that an increase in the likelihood of failure increase the likelihood of CCF is not correct; CCF likelihood is increased only when independence is reduced through shared resources (i.e., hardware or design) and the likelihood of failure in that shared resource is not "sufficiently low". Even when the likelihood of failure is not "sufficiently low", if the likelihood of failure is still significantly lower than a single random hardware failure, the CCF is so unlikely that "best-estimate" analysis as a beyond design basis event is appropriate, as defined in the SRM to SECY 93-087, BTP 7-19 and NEI 01-01. Alternately, if the likelihood of failure is not significantly lower than a single random hardware failure, conservative analysis as a design basis event is appropriate.

    Similarly, on Attachment page 5, Item 2, the statement that reducing the level of diversity, separation or independence increases malfunction likelihood to be "more than minimal increase" is not correct. These reductions increase CCF likelihood, but if the CCF is only due to a design defect, and the CCF likelihood is still significantly lower than a single hardware failure (i.e., there is a robust design process), then the malfunction likelihood is still acceptable for a favorable answer to 50.59 Question ii.

13. Attachment, page 5, Note – The first sentence incorrectly refers to integration of hardware and software; all digital designs integrate hardware and software; there is nothing problematic about that. The problem is integration of design functions.

14. Attachment, page 5, Item 3 - This incorrectly mixes likelihood with malfunction results. Here are a few examples to illustrate the problem:

a) A very simple relay, that has an MTBF of 10 years, can be replaced by a different very simple relay, that has an MTBF of 5 years. This simplicity precludes consideration of a new malfunction result due to a CCF caused by a design defect, regardless of where else that new relay is used (i.e., the CCF likelihood is "sufficiently low", which yields a favorable answer for 50.59 Question vi). But this CCF prevention cannot compensate for the fact that the new relay has a higher likelihood of failure than the old relay (i.e., an unfavorable answer for 50.59 Question ii).

b) Two separate analog controllers controlling two feedwater pumps are replaced by two separate digital controllers that have the potential for CCF due to a common digital design defect. To prevent a CCF, due to a design defect that leads to an unanalyzed excess feedwater event (overcooling), you can add internal diversity to each digital controller, with a 2oo2 output configuration; this facilitates a favorable answer to 50.59 Question vi (i.e., the CCF likelihood is now "sufficiently low"). But if the combined reliability of the two diverse digital components is less than the one original analog component, the likelihood of a malfunction that can lead to a loss of a feedwater pump has increased; this results in an unfavorable answer to 50.59 Question ii.

c) EFW isolation valves typically have two safe states – open for a loss of feedwater event, closed for a ruptured steam generator event. If you install diverse controllers in a 1oo2 configuration to ensure the valves will open, then a failure in either diverse component will prevent the valves from closing; therefore, in preventing a CCF to ensure valve opening (i.e., a favorable answer for 50.59 Question vi), you have increased the likelihood of failure of the design function to close the valves (i.e., an unfavorable answer for 50.59 Question ii).

These examples illustrate why malfunction likelihood and malfunction results are two separate questions in 50.59. Both must be evaluated independently to facilitate a 50.59 digital upgrade.

15. Attachment, Section 3.1.1, second paragraph – Clarify that 'preventing failure from occurring' can be equated to "sufficiently low" likelihood, but 'limiting failures' cannot. Limitation only makes the results of a failure acceptable; it does not reduce the likelihood of the malfunction. Therefore, limiting design features do not contribute to dependability. In fact, they can adversely affect dependability. For example, adding more controllers to achieve more segmentation and thereby limit a CCF, reduces MTBF, which reduces dependability.

16. Table 1 – The design attribute "failure state always known to be safe" is correct in theory, but never in practice. Although we can predict failure states for specific conditions (e.g., loss of power), we can never guarantee that failure state, because we can never predict all potential failure sources. This is why, even though we design the RTS for fail-safe reactor trip, we cannot guarantee that, so we analyze and provide diverse mitigation for ATWS.

    Regardless, these fail-safe attributes are limiting measures that ensure an acceptable malfunction. They are completely unrelated and have no effect (positive or negative) on malfunction likelihood. A fail-safe design that achieves that is more likely to reach that failure state than its analog predecessor yields an unfavorable answer to 50.59 Question ii.

17. Section 4.3 – Uses the word "implausible". Do not introduce a new term; replace with "sufficiently low".

18. Attachment page 12 first paragraph - Internal diversity does more than "help to minimize the potential"; as defined in BTP 7-19, it precludes the need for further consideration of a CCF.

19. Section 4.4 – The RIS should clarify that digital upgrades should comply with current NRC criteria for digital technology; justifications for non-compliance to criteria for safety systems/components should be documented in the Qualitative Assessments. In that regarding, BTP 7-19 Revision 6 supersedes NEI 01-01; its D3 analysis criteria is applicable to RTS, ESFAS, ESF auxiliary supporting features, and any safety function that is credited in the safety analysis to respond to the DBE, where a further

consideration of a CCF is needed. The BTP 7-19 D3 analysis criteria is not applicable to safety systems where a CCF is precluded through simplicity or internal diversity.

20. Table 2 Step 2 - Change to "Consider the possibility that the proposed modification may have introduced potential **new** failures."

21. Table 2 Step 2, first bullet – Add (e.g., spurious actuation, **erroneous control**); this is needed because the potential for erroneous control is too often overlooked.

22. Section 3 – A list of characteristics that are likely to result in a "sufficiently low" conclusion, implies that other characteristics are not acceptable to reach a "sufficiently low". This section should be replaced by characteristics that have the potential to cause new malfunctions (i.e., shared digital components, interconnected digital components, digital components that have common design blocks) and examples of design attributes that can prevent these new malfunctions, and thereby facilitate a "sufficiently low" conclusion. The RIS should be explicitly clear where these examples must be replaced by specific attributes, such as simplicity and diversity for safety functions credited for DBE mitigation.

23. The RIS is currently silent on 50.59 question iii "Result in more than a minimal increase in the consequences of an accident previously evaluated in the final safety analysis report". The RIS should be very clear that a digital failure that affects multiple divisions of a safety function credited for accident mitigation, such as a CCF due to a design defect, can increase the consequences of an accident.

24. The RIS should be clear that "accidents" in 50.59 questions i and v encompass anticipated operational occurrences (AOO). Digital failures can increase the frequency of AOOs, and when the "sufficiently low" threshold is not reached, digital CCFs can cause new AOOs. This clarification in the RIS will correct an industry misunderstanding that I&C systems cannot cause accidents.