NRR-DMPSPEm Resource

From: Ken Scarola <KenScarola@NuclearAutomation.com>
Sent: Thursday, March 08, 2018 1:53 PM
To: Govan, Tekia
Cc: Carte, Norbert; Rahn, David; Chernoff, Harold; Thomas, Brian; Morton, Wendell
Subject: [External_Sender] Comments on Draft RIS 2002-22 Supplement 1
Attachments: 2018-03-08 NAE Comments on Draft RIS provided for 2018-03-06 NRC meeting.docx

Tekia,
Attached are my comments on the draft RIS that was discussed at the 2018-03-06 Category 3 meeting. This attachment documents the comments I made at the meeting (with more clarity); it also includes a few more comments that were not discussed due to the time constraint. Please distribute these comments to other NRC attendees whose emails I did not have.

I'm hopeful the Staff will allow further discussion on these topics at the next Category 3 meeting, 2018-03-14, which I am planning to attend.

Thank you for the opportunity to contribute to this extremely important industry effort.

Ken

Ken Scarola
Nuclear Automation Engineering, LLC
3672 Pine Tree Ln.
Murrysville, PA 15668
412-612-1192

Hearing Identifier: NRR_DMPS
Email Number: 243

Mail Envelope Properties (008601d3b70e$b0c10020$12430060$)

Subject: [External_Sender] Comments on Draft RIS 2002-22 Supplement 1
Sent Date: 3/8/2018 1:52:57 PM
Received Date: 3/8/2018 1:53:49 PM
From: Ken Scarola

Created By: KenScarola@NuclearAutomation.com

Recipients:
"Carte, Norbert" <Norbert.Carte@nrc.gov>
Tracking Status: None
"Rahn, David" <David.Rahn@nrc.gov>
Tracking Status: None
"Chernoff, Harold" <Harold.Chernoff@nrc.gov>
Tracking Status: None
"Thomas, Brian" <Brian.Thomas@nrc.gov>
Tracking Status: None
"Morton, Wendell" <Wendell.Morton@nrc.gov>
Tracking Status: None
"Govan, Tekia" <Tekia.Govan@nrc.gov>
Tracking Status: None

Post Office: NuclearAutomation.com

Files	**Size**	**Date & Time**
MESSAGE	785	3/8/2018 1:53:49 PM
2018-03-08 NAE Comments on Draft RIS provided for 2018-03-06 NRC meeting.docx	26598	

Options

Priority:	Standard
Return Notification:	No
Reply Requested:	No
Sensitivity:	Normal
Expiration Date:	
Recipients Received:	

Comments on DRAFT NRC REGULATORY ISSUE SUMMARY 2002-22, SUPPLEMENT 1 provided for 2018-03-06 Category 3 meeting – Ken Scarola, Nuclear Automation Engineering

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 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 the Qualitative Assessment requires an engineering evaluation.

   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 Assessment are clearly explained in Section 3, along with performance under the licensee's NRC approved quality assurance program. This would better reflect the actual industry practice, where the Qualitative Assessment is most often conducted as part of the engineering process.

2. The RIS gives licensees the discretion to determine what design attributes can be credited 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") 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".

   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'.

   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 required to reach the "sufficiently low" threshold.

   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 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.

Please note that changing the criteria 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 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".

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.

It is also noted that the lack of excluding ESF auxiliary supporting features on page 2 is inconsistent with the Attachment, page 5, Item 1(c), where ESF control logic and load sequencers are implicitly excluded from the RIS.

3. NRC and industry have both identified screening as a key source of 50.59 errors and inconsistency throughout the industry. 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 likelhood, 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 required to preclude evaluation of any potential malfunctions when answering questions v and vi. Therefore, if the Qualitative Assessment 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 three 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.
   b) Failure likelihood is not "sufficiently low", but no more than a marginal increase compared to its analog predecessor – a malfunction result evaluation is needed for 50.59 Questions v and vi.
   c) Failure likelihood 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 paragraph) 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.

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 Assessment, because these malfunctions are significantly less likely than malfunctions due to single random hardware failure. The RIS should clarify this point.

However, the RIS should also clarify that malfunctions due to a random failure of a shared hardware resource 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, and how those differences are applied when analyzing malfunctions for initiators vs. mitigators (e.g., concurrent events that must be considered, equipment and manual actions that can be credited for mitigation, acceptance criteria).

If the RIS does not consider a malfunction due to a design defect to be a beyond design basis event, 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), 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 to be analyzed as a beyond design basis event also creates 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".

6. 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.

7. ML13298A787, November 5, 2013 identifies many issues that have plagued digital upgrades. To avoid continued industry confusion, this RIS needs to 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" (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 UFSAR". Due to the inherent complexity of 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), 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 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).

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, or when the same digital design is used for multiple design functions. Any type of integration (through shared/interconnected hardware or shared design) creates a CCF vulnerability (Attachment, page 5, item 1(a)); the purpose of the Qualitative Assessment is to demonstrate that the vulnerability is "sufficiently low" to require no further malfunction results analysis for 50.59 Questions v and vi.

    The RIS should clarify that 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. 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 Assessment 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.

    The RIS should clarify that when the same digital design is used for multiple design functions, that digital design is a shared resource, whose failure can adversely and concurrently affect those design functions. When performing the Qualitative Assessment 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.

    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 the CCF requires no further malfunction consideration.

    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 cause unanalyzed transients. These CCFs may not affect SSCs credited in the UFSAR for accident mitigation and they may be within the same echelon of defense (contrary to the statements in Attachment Section 4.2.2); regardless, unanalyzed transients are of equal concern.

11. Page 2, paragraph 2 – Change RPS to RTS, because RPS encompasses RTS and ESFAS.

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 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".

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", therefore 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., 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.

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" it precludes the need for further consideration of a CCF.

19. Section 4.4 – Digital upgrades should comply with current NRC criteria for digital technology. In that regarding, BTP 7-19 supersedes NEI 01-01; it requires a D3 analysis for RTS, ESFAS, ESF auxiliary supporting features, and any safety function that is credited in the safety analysis to respond to the DBE, where a CCF requires further consideration. BTP 7-19 does not require a D3 analysis 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.