June 15, 2018

MEMORANDUM TO: Harold K. Chernoff, Branch Chief
ROP Support and Generic Communications Branch
Division of Inspection and Regional Support
Office of Nuclear Reactor Regulation

FROM: Tekia Govan, Project Manager ***/ra/***
ROP Support and Generic Communications Branch
Division of Inspection and Regional Support
Office of Nuclear Reactor Regulation

SUBJECT: RESPONSE TO PUBLIC COMMENTS ON DRAFT REGULATORY ISSUE SUMMARY 2002-22, SUPPLEMENT 1, "CLARIFICATION ON ENDORSEMENT OF NUCLEAR ENERGY INSTITUTE GUIDANCE IN DESIGNING DIGITAL UPGRADES IN INSTRUMENTATION AND CONTROL SYSTEMS"

The U.S. Nuclear Regulatory Commission (NRC) issued a notice of opportunity for public comment on the subject draft regulatory issue summary (RIS) in Volume 83 of the *Federal Register*, page 11154 (83 FR 11154), on March 14, 2018. The notice provided a 15-day comment period. Seven organizations and individuals provided comments, which the NRC staff considered before issuing the final RIS. The NRC received comments from the Nuclear Energy Institute (Agencywide Documents Access and Management System (ADAMS) Accession No. ML18088A158), Norbert Carte (ADAMS Accession No. ML18088A307), Kenneth Scarola (ADAMS Accession Nos. ML18092A074 and ML18092A075), Tennessee Valley Authority (ADAMS Accession No. ML18092A076), and anonymous submittals (ADAMS Accession Nos. ML18088A304, ML18088A306, and ML18088A308). The staff's responses to all public comments are enclosed.

Enclosure:
As stated

CONTACT: Tekia Govan, NRR/DIRS/IRGB
301-415-6197

RESPONSE TO PUBLIC COMMENTS ON DRAFT REGULATORY ISSUE SUMMARY 2002-22, SUPPLEMENT 1, "CLARIFICATION ON ENDORSEMENT OF NUCLEAR ENERGY INSTITUTE GUIDANCE IN DESIGNING DIGITAL UPGRADES IN INSTRUMENTATION AND CONTROL SYSTEMS," Date: June 15, 2018

ADAMS Accession Nos.: ML18115A298 *concurred via e-mail

OFFICE	QTE*	NRR/DIRS/IRGB/LA*	OGC*	NRR/DE/EICB/BC
NAME	KAzariah-Kribbs	ELee	SClark	MWaters (RAlvarado for)
DATE	05/10/2018	05/30/2018	06/13/2018	06/14/2018
OFFICE	NRR/DIRS/IRGB/PM	NRR/DIRS/IRGB/BC		
NAME	TGovan	HChernoff		
DATE	06/14/2018	06/15/2018		

OFFICIAL RECORD COPY

Analysis of Public Comments on
DRAFT NRC REGULATORY ISSUE SUMMARY 2002-22, SUPPLEMENT 1
"CLARIFICATION ON ENDORSEMENT OF NUCLEAR ENERGY INSTITUTE GUIDANCE IN DESIGNING DIGITAL UPGRADES IN INSTRUMENTATION AND CONTROL SYSTEMS"

Comments on the subject draft regulatory issue summary (RIS) are available electronically at the U.S. Nuclear Regulatory Commission's (NRC's) electronic Reading Room at http://www.nrc.gov/reading-rm/adams.html. From this page, the public can access the Agencywide Documents Access and Management System (ADAMS), which provides text and image files of the NRC's public documents. The following table lists the comments the NRC received on the draft RIS.

Letter Number	ADAMS Accession No.	Commenter Affiliation	Commenter Name
1	ML18088A158	Nuclear Energy Institute	Jerud Hanson
2	ML18088A304	No Known Affiliation	Anonymous (1)
3	ML18088A306	No Known Affiliation	Anonymous (2)
4	ML18088A307	U.S. Nuclear Regulatory Commission	Norbert Carte
5	ML18088A308	No Known Affiliation	Anonymous (3)
6	ML18092A074	Nuclear Automation Engineering, LLC	Kenneth Scarola
7	ML18092A075	Nuclear Automation Engineering, LLC	Kenneth Scarola
8	ML18092A076	Tennessee Valley Authority	Chris Riedl and J.W. Shea

This document lists each public comment by letter number, as given in the table above. The original comment as written by the commenter is listed first, followed by the NRC's response. In some instances, the comment is broken into segments for clarity. In that case, each comment within the corresponding letter is also given a sequential comment number. It should be noted that Commenter 1, Nuclear Energy Institute (NEI) submitted its comments in a table with references to a "track changed" version of the RIS to illustrate how the commenter would like the RIS to be revised.

Letter 1—Comments from the Nuclear Energy Institute

Comment No. 1-1

Recommended Change
Page No. 2 of 5
Suggest revising the Intent Section, third paragraph as proposed in revised RIS included with comment spreadsheet.

Justification

(a) *Stating that DI&C upgrades associated with the RPS/ESFAS are out-of-scope for the RIS Supplement has the potential to communicate that SSCs supporting or actuated by the RPS/ESFAS logic would also be off the table. This change clarifies the scope.*

(b) *Additionally, this paragraph states, in part, "This RIS does not provide ... guidance for addressing common cause failure ... Additional guidance for addressing potential common cause failure of digital I&C equipment is contained in other NRC guidance*

documents and NRC-endorsed industry guidance documents." Page 1 of 17 (second to last paragraph) of the RIS attachment states "Thus, the 'qualitative assessment' provides a means of addressing software CCF." The statement provided in the Intent Section would seem to contradict the statement made on page 1 of 17 of the RIS attachment.

NRC Response

(a) The NRC staff agrees with this comment. The staff revised the Intent section of the RIS and Section 3 of the RIS attachment to clarify the type of modifications that are within scope of the RIS.

(b) The NRC staff agrees with this comment. The Intent section of the RIS has been revised to clarify that the RIS provides a method for addressing common cause failure (CCF) for 10 CFR 50.59 evaluations.

Comment No. 1-2

Recommended Change
Page No. 3 of 5
Summary of Issue Section: Suggest deleting the first two sentences of the first paragraph of this section as proposed in revised RIS included with comment spreadsheet.

Additionally, it would be appropriate to switch the order of the first two paragraphs of this section to provide a better flow of information.

Justification
The first paragraph sends an unbalanced message to the public and other stakeholders, implying that digital modifications are adverse to safety.

NRC Response
The NRC staff agrees with this comment. The staff revised the Summary of Issues section of the RIS to provide a more balanced message regarding the impact of digital modifications.

Comment No. 1-3

Recommended Change
Page No. 5 of 5
Very last statement in the RIS front matter: Suggested rewording as proposed in revised RIS included with comment spreadsheet for "Qualitative Assessment and Engineering Evaluation Framework."

Justification
The RIS Supplement should only provide guidance on development of a Qualitative Assessment framework.

NRC Response
The NRC staff disagrees with this comment. However, the staff removed the term “Engineering Evaluation” from the title and revised it to, “Qualitative Assessment and Failure Analysis.” This title is consistent with the revisions to the RIS as a result of public comments.

Comment No. 1-4

Recommended Change
Page No. 1 of 17
RIS Supplement Attachment: Suggested wording proposed in revised RIS included with comment spreadsheet for changing the title of the attachment from "Qualitative Assessment and Engineering Evaluation Framework" to "Qualitative Assessment Framework."

Justification
Comment 20 (page 10 of 17) recommends deletion of Section 4: Engineering Evaluation" in its entirety.

NRC Response
The NRC staff disagrees with this comment. The staff revised Section 4 of the attachment to the RIS to provide guidance on failure analysis. The staff also revised the title of Section 4 in the RIS to "Engineering Evaluation: Failure Analysis."

Comment No. 1-5

Recommended Change
Page No. 1 of 17
RIS Supplement Attachment, Section 1, Purpose (third paragraph) -Suggest deleting this paragraph and removing "Dependability Evaluation" as proposed in revised RIS included with comment spreadsheet.

Justification
Introduction of the term "Dependability Evaluation" is not beneficial and could cause confusion. The RIS should only provide guidance on development of a qualitative assessment. With the addition of dependability assessments, a licensee will assume that two new documents will need to be produced.

NRC Response
The NRC staff disagrees with this comment. NEI 01-01 defines the term "Dependability Evaluation." The staff revised the paragraph for clarity to address the concern expressed.

Comment No. 1-6

Recommended Change
Page No. 1 of 17
RIS Supplement Attachment, Section 1, Purpose, fourth paragraph: Suggest deleting this sentence as proposed in revised RIS included with comment spreadsheet.

Justification
Last sentence of the fourth paragraph seems out of place with the paragraph discussion.

NRC Response
The NRC staff disagrees with this comment. No changes were made to the RIS.

Comment No. 1-7

Recommended Change
Page No. 2 of 17
RIS Supplement Attachment, Section 2 (second paragraph): Replace "adverse" with "negative' in the document as proposed in revised RIS included with comment spreadsheet.

Justification
"Adverse" has a distinct meaning in the 50.59 screening process. The use of adverse in the RIS does not line up with the meaning of adverse in 50.59 and is not necessary here.

NRC Response
The NRC staff agrees with this comment. The staff revised Section 2 of the RIS as suggested in the recommended change.

Comment No. 1-8

Recommended Change
Page No. 2 of 17
RIS Supplement Attachment, Section 2.1, regarding the statement "This 'sufficiently low' threshold is not interchangeable with that for distinguishing between events that are 'credible' or 'not credible'. Suggest deleting this statement as proposed in revised RIS included with comment spreadsheet.

Justification
The threshold for determining whether an event is credible or not is whether it is 'as likely as' (i.e., not 'much lower than') malfunctions already assumed in the [updated final safety analysis report] UFSAR." This statement is irrelevant to the discussion and may cause confusion. In addition, the terms "credible" and "not credible" are not used anywhere else in the document.

NRC Response
The NRC staff disagrees with this comment. The sentence is necessary to eliminate confusion when using the term “credible” to describe likelihood thresholds of 10 CFR 50.59. “Credible” is not an outcome under the qualitative assessment. The staff made no changes to the RIS based on this comment.

Comment No. 1-9

Recommended Change
Page No. 3 of 17
RIS Supplement Attachment, Section 2.1: "For digital modifications, particularly those that introduce software, there may be the potential increase in likelihood of failure, including a single failure. For redundant SSCs, this potential increase in the likelihood of failure creates a similar increase in the likelihood of a common cause failure." Suggest deleting this statement as proposed in revised RIS included with comment spreadsheet.

Justification
There is no basis for declaring that the potential for single CCF is directly proportional to the potential increase in likelihood of failure, as not all failures are common cause and the statement is unnecessary. In practice, the introduction of digital equipment has proven to

decrease the likelihood of failure due to such things as elimination of single points of vulnerability and self diagnostics.

NRC Response
The NRC staff disagrees with this comment. The sentence is accurate in its description of the potential for an increased likelihood of a failure that could occur due the introduction of software. The staff made no changes to the RIS based on this comment.

Comment No. 1-10

Recommended Change
Page No. 3 of 17
RIS Supplement Attachment, Section 2.1: Suggest rewording as proposed in revised RIS included with comment spreadsheet. Note that the proposed Criteria wording consolidates the wording provided on Lines 369 through 442. Therefore, it is also suggested that Lines 369 through 442 be deleted.

Justification
Criteria, conflicts with language in 96-07, Appendix D.

NRC Response
The NRC staff disagrees with this comment. The content of the proposed NEI 96-07, Appendix D, is beyond the scope of the RIS. The staff made no changes to the RIS based on this comment.

Comment No. 1-11

Recommended Change
Page No. 4 of 17
RIS Supplement Attachment, Section 3 for Qualitative Assessments: Suggest rewording as proposed in revised RIS included with comment spreadsheet.

Justification
[(a)] Item (1) will be interpreted by licensees such that a non-safety related digital control system would require a LAR to implement and would also prevent a licensee from a simple one-for-one replacement of analog/pneumatic sequencer timing relays with modern timing relays containing an embedded digital device.

[(b)] Item (2) addresses a reduction in redundancy, diversity, separation or independence. If these attributes are design features rather than design or regulatory requirements, it may not be necessary to maintain that level of UFSAR described redundancy, diversity, separation, or independence. In other words, if these are not "credited" then maintaining those design features may not be required. This is particularly true for non-safety related systems, where these attributes are not typically required.

[(c)] Item (3) reintroduces 100% testing which is not achieved with software and then introduces an input/output state analysis. Licensees will assume this requirement applies to non-safety related equipment as well as safety related equipment.

NRC Response
The NRC staff agrees with this comment. The staff revised Section 3 of the RIS to provide examples of proposed digital instrumentation and control (I&C) modifications that could readily be implemented without prior NRC approval (e.g., modifications to non-safety related systems). In addition, the staff removed the discussion of 100 percent testing. Although the staff agrees with this comment, the commenter provided suggested wording that was not used by the staff to revise Section 3.

Comment No. 1-12

Recommended Change
Page No. 6 of 17
RIS Supplement Attachment, Section 3.1.1: Consider striking "need to" in the following statement: "However, design features external to the proposed modification (e.g., mechanical stops on valves) may also need to be considered." Suggested wording as proposed in revised RIS included with comment spreadsheet.

Justification
Current wording would indicate a directive rather than an optional consideration.

NRC Response
The NRC staff agrees with the comment. The staff revised Section 3.1.1 of the RIS to remove the words “need to.”

Comment No. 1-13

Recommended Change
Page No. 6 of 17
RIS Supplement Attachment, Section 3.1.1 Suggest deleting last sentence in 3.1.1 as proposed in revised RIS included with comment spreadsheet.

Justification
Sentence is unnecessary as commentary and could potentially be confusing.

NRC Response
The NRC staff disagrees with the comment. The staff made minor edits to Section 3.1.1 of the RIS to clarify the diversity discussion.

Comment No. 1-14

Recommended Change
Page No. 7 of 17
RIS Supplement Attachment, Section 3.1.2 - Quality of the Design Process - Suggest rewording as proposed in revised RIS included with comment spreadsheet for Section 3.1.2. Quality of the Design Process.

Justification
Licensees will interpret the guidance provided in this section in a way that concludes non-safety related equipment must now comply with industry standards.

NRC Response
The NRC staff agrees with the comment. The staff revised Section 3.1.2 of the RIS to provide guidance that specifically addresses non-safety related equipment.

Comment No. 1-15

Recommended Change
Page No. 7 of 17
RIS Supplement Attachment, Section 3.1.3, Operating Experience - See the proposed revised RIS included with the comment spreadsheet for suggested changes to Section 3.1.3, Operating Experience.

Justification
The language in this section is focused on applicability with specific sited references or evidence. At the site inspection level, this type of language would appear to focus on traceability of documented evidence rather than evaluating and using operating history to inform the design. Vendors will not usually provide names of customers associated with a given problem report. Thus, traceability or specific references to environmental conditions and other design attributes are not generally possible to obtain. Also, the guidance does not provide a clear expectation of what the use of operating experience is to accomplish.

NRC Response
The NRC staff disagrees with this comment and did not incorporate the suggested edits. The staff believes that the proposed edits would unnecessarily restrict the use of operating experience in support of qualitative assessments. Licensees have discretion in determining how to apply operating experiences in the development of qualitative assessments. The staff made no changes to the RIS based on this comment.

Comment No. 1-16

Recommended Change
Page No. 9 of 17
RIS Supplement Attachment, Table 1 - See the proposed revised RIS included with the comment spreadsheet for suggested changes to Table 1.

Justification
[(a)] In the first category, some of the guidance is not achievable.
[(b)] The second category does not distinguish between safety and non-safety requirements.
[(c)] In the third category, OE was revised to align with the revised section of OE.

NRC Response
The NRC staff agrees with this comment. The staff revised Table 1 of the RIS in a manner consistent with the theme of the comment.

Comment No. 1-17

Recommended Change
Page No. 10 of 17
RIS Supplement Attachment, Section 4, Engineering Evaluations - Suggest deletion of Section 4 in its entirety as proposed in revised RIS included with comment spreadsheet.

Justification
Licensees already have very detailed and proceduralized digital design guidance along with a quality assurance program. There is also an effort underway to standardize on an industry digital I&C design process.

NRC and licensees have not been fully aligned on adequate documentation of the design considerations employed in a proposed digital activity. The new RIS should provide licensees with acceptable methods for developing qualitative assessments in a way that an inspector can understand pertinent design considerations. Therefore, the new RIS should focus only on development and documentation of qualitative assessments and should not provide digital I&C design guidance.

NRC Response
The NRC staff agrees, in part, with this comment. The staff is not providing detailed design guidance in this RIS and expects licensees to use the design process in their NRC-approved Quality Assurance Program. Consistent with NEI 01-01, Section 5.1, failure analysis is an integral part of the design process and provides information to support licensing evaluations. It also provides a means of documenting resolution of identified potential failures. The staff revised Section 4 of the RIS to clarify how potential CCF vulnerabilities can be addressed through failure analysis and documented in the final design.

Comment No. 1-18

Recommended Change
Page No. 14 of 17
RIS Supplement Attachment, Figure 1 - Suggest deletion of Figure 1 as proposed in revised RIS included with comment spreadsheet.

Justification
The process outlined in Figure 1 blurs the line between a dependability evaluation and a qualitative assessment. Figure 1 suggests only a dependability evaluation is needed. Figure 1 does not mention qualitative assessment, although the supporting information listed in Figure 1 is the supporting information that makes up a qualitative assessment. In short, Figure 1 adds confusion to the process.

The RIS should only provide guidance on development of a qualitative assessment for evaluating equipment/SSC reliability and CCF susceptibility.

NRC Response
The NRC staff agrees with the removal of the figure. While consistent with the process described in NEI 01-01, the figure did not provide an additional clarification beyond the guidance that is provided in NEI 01-01. The staff removed Figure 1 from the RIS.

Comment No. 1-19

Recommended Change
Page No. 15 of 17
RIS Supplement Attachment, Table 2 - Suggest deleting Table 2 in its entirety as proposed in revised RIS included with comment spreadsheet since most of these questions are covered in NEI 01-01.

Justification
Table 2 contains approximately 22 questions. NEI 01-01 Appendix A contains an additional 42 questions that licensees already address when developing a 50.59 Evaluation for digital plant changes. The majority of Table 2 are already covered by the questions in NEI 01-01 Appendix A. However, licensees will feel obligated to address each Table 2 question individually in addition to the 42 NEI 01-01 Appendix A questions.

NRC Response
The NRC staff disagrees with deleting Table 2. The staff modified Table 2 to reflect the revised Section 4 of the RIS, which focuses on failure analysis documentation. Changes to Table 2 incorporated feedback that was discussed during a March 14, 2018, public meeting.[1]

Comment No. 1-20

Recommended Change
The proposed revised RIS included with the comment spreadsheet contains various editorial changes to specify that hardware within the scope of the RIS is limited to hardware on which software resides or hardware which has been programmed using software (i.e., hardware that contains a programmable logic device).

Justification
The draft RIS Supplement addresses digital hardware and software. Industry is concerned that new digital hardware requirements may be implied by the RIS. Digital hardware should not be treated differently than analog hardware. Analog hardware is not subject to an analysis of CCF and likewise digital hardware should not be subject to an analysis of CCF. The draft RIS may lead some to believe that a CCF analysis of digital hardware is a requirement.

NRC Response
The NRC staff disagrees with this comment. The need for evaluating the potential for CCF is not technology specific.

Letter 2—Comments from Anonymous (1)

Comment No. 2-1

Please provide more time to comment on this document. 15 days is not sufficient to digest this complex and convoluted document. There are several ways that this document is inconsistent with the intent of the rule of past practices.

NRC Response
The NRC staff disagrees with this comment. The NRC published a notice of opportunity for public comment on this RIS in the *Federal Register* on July 3, 2017 (82 FR 30913). This comment period lasted for 45 days. The NRC published an additional notice of opportunity for public comment on this RIS in the *Federal Register* on March 14, 2018 (83 FR 11154). This was established at 15 days, in part, based on the previous opportunity for comment on this RIS.

[1] Public meeting minutes dated March 14, 2018 (ADAMS Accession No. ML18156A414)

Letter 3—Comments from Anonymous (2)

This document is inconsistent with the intent of the 50.59, as expressed in NRC communications to the public. The 1999 change to the 50.59 rule was meant as a relaxation to the rule in effect at that time (see 64 FR 53582). Prior to the change the 50.59 rule stated: "A proposed change, test, or experiment shall be deemed to involve an unreviewed safety question (i) if the probability of occurrence or the consequences of an accident or malfunction of equipment important to safety previously evaluated in the safety analysis report may be increased; or (ii) if a possibility for an accident or malfunction of a different type than any evaluated previously in the safety analysis report may be created; or (iii) if the margin of safety as defined in the basis for any technical specification is reduced."

In effect, the old (i) became the new (i)-(iv) and the old (ii) became the new (v) & (vi). The new rule states:
"(i) Result in more than a minimal increase in the frequency of occurrence of an accident previously evaluated in the final safety analysis report (as updated);
(ii) Result in more than a minimal increase in the likelihood of occurrence of a malfunction of a structure, system, or component (SSC) important to safety previously evaluated in the final safety analysis report (as updated);
...
(v) Create a possibility for an accident of a different type than any previously evaluated in the final safety analysis report (as updated);
(vi) Create a possibility for a malfunction of an SSC important to safety with a different result than any previously evaluated in the final safety analysis report (as updated);"

One point to derive form the above is that Questions (i)-(iv) were intended to evaluate the impact of a change on accidents and malfunctions that were previously evaluated in the UFSAR. Furthermore, Questions (v) and (vi) were intended to evaluate any new or different accidents and malfunctions that were created as a result of the change.

The primary concern of the Supplement to RIS 2002-22 is to provide guidance on how to address digital CCF. This first step must be to determine whether the digital CCF is just a new initiator for an existing accident or malfunction, or a new accident or malfunction. Then the most applicable 50.59 evaluation questions must be identified. Finally the criteria of the applicable questions must be identified and applied (e.g., frequency or likelihood of occurrence, consequences, types of design basis accidents and AOOs, or malfunction results).

Obviously, more than one question can be applicable to any change (and all questions must be answered for each change), but each accident or malfunction would either be addressed by Questions (i)-(iv) or (v) & (vi).

Generally, if an existing digital system (or component) is replaced with a new one of the same scope, capability, and connections, then digital CCF should be addressed by Questions (i)-(iv); however, if an existing analog system (or component) is replaced by a digital one, and particularly if the new one is NOT of the same scope, capability, and connections as the old one, then Questions (v) & (vi) may be needed to address digital CCF. Obviously, the most applicable evaluation question is determined by the specific changes and the resultant changes in accidents or malfunctions.

Generally, digital CCF is not a concern for impacting the likelihood of accidents or malfunction that were previously evaluated in the UFSAR; that is, new digital equipment is generally more

reliable than the equipment it is replacing. The "sufficiently low" criteria is not needed to address these (i.e., not needed for Questions (i) and (ii)). Please remove the new guidance for "sufficiently low" from being applicable to Questions (i) and (ii).

Generally, digital CCF can create (by introducing newly shared resources, and coupling or combining previously distinct SSCs): (1) the possibility for new types of accidents, and/or (2) malfunctions with different results; to meet the "sufficiently low" criteria for these accidents and malfunctions, design attributes must be used. The RIS must state this clearly. Subsequently, in another document, the NRC must ensure guidance is published and/or endorsed that identifies acceptable design attributes for eliminating digital CCF from further consideration (e.g., updated BTP 7-19 Section 1.9). To publish guidance that something can be done, but not at least one acceptable way to do it, creates regulatory uncertainty. Furthermore, the lack of specific guidance on at least one acceptable approach makes it very difficult for an inspector to write a violation (or a licensee to ensure they will not get a violation).

NRC Response
The NRC staff disagrees with this comment. This RIS supplement provides clarification and no new positions are taken with regard to 10 CFR 50.59. Further, this RIS provides one acceptable method to address CCF in digital I&C modifications under 10 CFR 50.59 evaluations (i.e., sufficiently low). In particular, this RIS provides clarification on the use of qualitative assessments to make a determination of “sufficiently low” to address 10 CFR 50.59 (c)(2)(i), (ii), (v), and (vi). Guidance for addressing the effects of malfunctions/accidents is beyond the scope of this RIS. Sections 3 and 4 of the RIS state, in part, that incorporation of appropriate design attributes can help ensure that a proposed modification does not introduce reductions in redundancy, diversity, separation, or independence of UFSAR-described design functions.

NEI 96-07, Section 4.3.2, explains that a change that reduces system/equipment redundancy, diversity, separation, or independence (i.e., such that the UFSAR-described “design functions” would not be accomplished as “credited in the safety analyses”) requires prior NRC approval because it would result in more than a minimal increase in the likelihood of occurrence of a “malfunction of an SSC important to safety.” The RIS was revised to state that an adequate qualitative assessment of the likelihood of failure of a proposed modification would describe the specific design attributes incorporated to resolve the identified potential failures.

To the extent that this comment addresses the need for additional guidance for qualitative assessments, additional guidance documents for qualitative assessments are beyond the scope of this RIS (e.g. BTP 7-19).

Letter 4—Comments from Norbert Carte

Comment No. 4-1

The NRC has a public internet site: www.nrc.gov. This site has a page to communicate to the public documents that are available for comment: https://www.nrc.gov/public-involve/doc-comment.html. This web page has an entry for Generic Communication: https://www.nrc.gov/public-involve/doc-comment.html#gencomm. This document (which is available for public comment) is not shown on that page. I am concerned that members of the public, who are not intimately involved in the RIS development were not made aware of this document being available for public comment. Please consistently notice generic communications on this page, or provide a link on this page to where you do.

NRC Response
The NRC staff agrees with this comment. The NRC issued a notice in the *Federal Register* (83 FR 11154) on March 14, 2018, announcing the availability of the RIS and a 15-day comment period. The RIS was made publicly available on the NRC's "Documents for Comment" Web page (https://www.nrc.gov/public-involve/doc-comment.html) under the topic of Rulemaking-Related Documents. The staff will review the format of the Web page to appropriately reflect recent changes in the categorization of a RIS as a rulemaking-related document.

Letter 5—Comments from Anonymous (3)

Comment No. 5-1

The RIS Supplement provides no useful guidance for what an engineer must do in order to avoid a violation. Furthermore, it does not resolve any of the issues the NRC or industry have identified with NEI 01-01. This RIS supplement should simply withdraw approval of NEI 01-01.

NRC Response
The NRC staff disagrees with this comment. This RIS is not intended to provide guidance for engineers to "avoid a violation." No specific examples of unresolved issues were provided by the commenter. The RIS provides an acceptable approach for using qualitative assessments when performing 10 CFR 50.59 evaluations of digital I&C modifications. Additionally, no rationale was provided for why NRC should withdraw its previous endorsement of NEI 01-01. There were no changes to the RIS based on this comment.

Letter 6—Comments from Kenneth Scarola

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.

NRC Response
No response is required. The NRC staff acknowledges this general comment and responded to the specific comments below.

Comment No. 6-1a

Specific Comments

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.

NRC Response
The NRC staff disagrees with this comment. The draft RIS described the distinction between qualitative assessments and engineering evaluations. This description was included to identify the part of the process supporting the 10 CFR 50.59 evaluations as distinguished from the part of the process supporting engineering evaluations. The order of the discussions in the draft RIS reflected the focus of the document on performing qualitative assessment associated with 10 CFR 50.59 evaluations. Further, the draft RIS included a discussion regarding the connection between qualitative assessment for 10 CFR 50.59 evaluations and engineering evaluations. Nevertheless, Section 4 of the RIS was revised to focus on failure analysis documentation, which should address the issue raised by the comment regarding the distinction between qualitative assessments and the evaluation discussed in Section 4.

Comment No. 6-1b

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[ed] 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.

NRC Response
The NRC staff disagrees with this comment. This RIS is not intended to provide guidance for engineers to "avoid a violation." No specific examples of unresolved issues were provided by the commenter. The RIS provides an acceptable approach for using qualitative assessments when performing 10 CFR 50.59 evaluations of digital I&C modifications.

The staff revised Section 4 of this RIS and deleted much of the text referenced in the comment. The revised Section 4 focuses on failure analysis and demonstrates the link between the qualitative assessment and failure analysis resolution.

Comment No. 6-2

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).

NRC Response
The NRC staff agrees, in part, with this comment. The RIS provides examples of design attributes that can be used for demonstrating "sufficiently low." Establishing consistency between NRC agency documents and expediting efforts to reach agreement between NRC and industry regarding these attributes is beyond the scope of this document. The staff notes that NEI 01-01 references BTP 7-19, Revision 4, rather than Revision 6. The staff made no changes to the RIS based on this comment.

The RIS supplement applicability is different than the applicability of BTP 7-19, Revision 4. BTP 7-19, Revision 4, focuses on RPS and ESFAS, whereas the RIS supplement focuses on safety

auxiliary systems and a small subset of RPS and ESFAS components. Therefore, the staff disagrees with the two alternatives provided by the commenter.

Comment No. 6-3

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.

NRC Response
The NRC staff disagrees with the comment. The intent of this RIS is to clarify guidance for qualitative assessments and documentation. Qualitative assessments are used only in the evaluation of a portion of 10 CFR 50.59. The concern regarding 10 CFR 50.59 screening in this comment is beyond the scope of the RIS.

The RIS was revised to state that the staff recognize the benefits of digital technology and that the use of digital technology does not always result in an increased likelihood of failure.

Comment No. 6-4

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.

NRC Response
The NRC staff agrees, in part, with the comment. The staff agrees that a determination of "sufficiently low," as described in the RIS supplement, demonstrates that 10 CFR 50.59(c)(2)(i), (ii), (v), or (vi) do not require a license amendment prior to implementing a change, and no further evaluation is required for these criteria. The staff also agrees if "sufficiently low" is not met, it does not prevent a change from being implemented under 10 CFR 50.59 without a license amendment. In such cases, the change being considered can be evaluated further against the more specific terms of the 10 CFR 50.59 criteria (e.g., 10 CFR 50.59(c)(2)(vi) includes two factors – one related to possibility of a malfunction and another to whether that malfunction has a different result than any previously evaluated in the UFSAR). However, this RIS supplement provides guidance only addressing the threshold of "sufficiently low" needed to support the 10 CFR 50.59 evaluation. The staff made no changes to the RIS based on this comment.

Comment No. 6-5a

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 10 CFR 50.59 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.

NRC Response

The NRC staff disagrees with this comment. Use of "best estimate" methods in 10 CFR 50.59 evaluations is limited to the subject of the previous use of such methods in the UFSAR. Unless the licensee's UFSAR already incorporates "best estimate" methods, it cannot use such

methods to evaluate different results than those previously evaluated in the UFSAR. The RIS was revised to clarify the use of "best estimate" methods.

Comment No. 6-5b

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."

NRC Response
The NRC staff disagrees with this comment. This RIS provides clarification for performing qualitative assessments based on existing guidance. This RIS does not introduce any new distinctions between new and operating plants. The NRC staff's integrated strategy to modernize the NRC's digital I&C regulatory infrastructure is beyond the scope of this RIS. The staff made no changes to the RIS based on this comment.

Comment No. 6-6a

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.

NRC Response
The NRC staff agrees with this comment. The staff revised Section 3 of the RIS attachment to incorporate this concept. The RIS now states, "Note that design attributes and the quality of the design process are interrelated (i.e., the quality of the design process assures the proper implementation of design attributes). As a result, these two factors will always be essential elements of a qualitative assessment. Operating experience in most cases can serve to compensate for weakness in the other two factors."

Comment No. 6-6b

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.

NRC Response
The NRC staff agrees with this comment. The staff revised the RIS and removed, in its entirety, Section 4.5, "Dependability Evaluations," from the RIS. Additionally, the staff revised Section 3

of the RIS to provide examples of proposed digital I&C modifications that could readily be implemented without prior NRC approval (e.g., modifications to non-safety related systems).

Comment No. 6-6c

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).

NRC Response
The NRC staff agrees, in part, with this comment. Although this RIS describes some of the issues identified in the reference document, the RIS was not intended to address all of the issues identified. The staff revised Section 3 of the RIS to clarify that design attributes and quality of the design process can be interrelated and are essential parts of the qualitative assessment and that operating experience can be used to augment design attributes and quality of the design process.

The intent of this RIS is to clarify guidance for qualitative assessments and documentation. Although this RIS describes some of the issues identified in the reference document, the RIS is not intended to address all of the issues identified in this comment. The concern expressed in this comment is beyond the scope of the RIS.

Comment No. 6-7

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.

NRC Response
The NRC staff disagrees with this comment. The intent of this RIS is to clarify guidance for qualitative assessments and documentation. Although this RIS describes some of the issues identified in the reference document, the RIS is not intended to address all of the issues identified in this comment. The concern expressed in this comment is beyond the scope of the RIS. The staff made no changes to the RIS based on this comment.

Comment No. 6-8

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).

NRC Response
The NRC staff disagrees with this comment. The examples within the definition of "sufficiently low" in NEI 01-01 are not all-inclusive. The staff does not agree that the examples pertain only to analog design flaws. The staff made no changes to the RIS based on this comment.

Comment No. 6-9

The NRC and industry focus on CCF due to software has led to confusion, because there are complex digital devices such as [field-programmable gate arrays] FPGAs and [programmable logic devices] 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.

NRC Response
The NRC staff disagrees with the comment. The staff's position is that FPGAs and PLDs are treated as software; therefore, it is not necessary to use "digital" or "digital design" exclusively. DI&C-ISG-04 states that "The contents and configuration of field programmable memory should be considered to be software, and should be developed, maintained, and controlled accordingly." The staff made no changes to the RIS based on this comment.

Comment No. 6-10a

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.

NRC Response
The NRC staff agrees with the first two paragraphs of this comment. The staff reviewed the RIS and believes it addresses the concerns noted in the comment. Section 4 of the RIS was revised to clarify the consideration of hazards in digital I&C modifications (e.g., modifications to non-safety related systems) related to combining design functions, interconnectivity between systems and digital communications.

With regard to the third paragraph of this comment, the RIS no longer references ISG-04. Use of other guidance documents is beyond the scope of this RIS. The staff made no changes to the RIS based on paragraph three of this comment.

The NRC staff acknowledges the comment in paragraph four. Sections 3 and 4 of the RIS state, in part, that incorporation of appropriate design attributes can help ensure that a proposed modification does not introduce reductions in redundancy, diversity, separation, or independence of UFSAR-described design functions. The RIS was revised to state that an adequate qualitative assessment of the likelihood of failure of a proposed modification would describe the specific design attributes incorporated to resolve the identified potential failures. The staff made no changes to the RIS based on paragraph four of this comment.

Comment No. 6-10b

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).

NRC Response
The NRC staff disagrees with this comment. The RIS was revised to state that the staff recognize the benefits of digital technology and that the use of digital technology does not always result in an increased likelihood of failure. The intent of this RIS is to clarify guidance for qualitative assessments and documentation. The concern expressed in this comment is beyond the scope of the RIS. The staff made no changes to the RIS based on this comment.

Comment No. 6-10c

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.

NRC Response
Although the NRC staff agrees with the first sentence of this comment, the staff disagrees with the remaining portion of the comment. Section 4 of the RIS was revised to clarify the consideration of hazards in digital I&C modifications (e.g., modifications to non-safety related systems) related to combining design functions, interconnectivity between systems and digital communications.
The staff made no changes to the RIS based on this comment.

Comment No. 6-11

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

NRC Response
The NRC staff disagrees with this comment. The staff's use of the term "reactor protection system" (RPS) is consistent with NEI 01-01, Section 5.2. The staff made no changes to the RIS based on this comment.

Comment No. 6-12a

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.

NRC Response
The NRC staff agrees with this comment. The RIS was revised to state that the staff recognizes the benefits of digital technology and that the use of digital technology does not always result in

an increased likelihood of failure.

Comment No. 6-12b

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."

NRC Response
The NRC staff disagrees with this comment. The RIS was revised to state that the staff recognizes the benefits of digital technology and that the use of digital technology does not always result in an increased likelihood of failure. For digital modifications, particularly those that introduce software, the likelihood of failure may potentially increase. For redundant SSCs, this potential increase in the likelihood of failure may create an increase in the likelihood of a CCF. The staff made no changes to the RIS based on this comment.

Comment No. 6-12c

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.

NRC Response
This comment addresses issues beyond the scope of the RIS. The scope of the RIS is limited to the documentation of sufficiently low determinations. The staff made no changes to the RIS based on this comment.

Comment No. 6-12d

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.

NRC Response
The NRC staff disagrees with this comment. As discussed in Section 4.3.2 of NEI 96-07, a reduction in these attributes is considered to be more than a minimal increase in the likelihood of a malfunction. However, in response to another public comment, the staff deleted the information from the RIS that is referenced in this comment.

Comment No. 6-13

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.

NRC Response
The NRC staff agrees that integration of design functions is a concern for digital I&C modifications. The RIS has been revised to emphasize this point.

Comment No. 6-14

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.

NRC Response
The NRC staff disagrees with this comment. The staff notes that the commenter does not reference a location in the RIS that illustrates the examples provided. However, NEI 96-07, Section 4.3.6, states, "…malfunctions with a different result are limited to those that are as likely to happen as those in the UFSAR." If a qualitative assessment determines that a potential failure (e.g., software CCF) has a sufficiently low likelihood, then the effects of the failure do not need to be considered in the 10 CFR 50.59 evaluation. Thus, the qualitative assessment provides a means of addressing software CCF. The staff made no changes to the RIS based on this comment.

Comment No. 6-15

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.

NRC Response
The NRC staff disagrees with this comment. The RIS is consistent with the concept of limiting the effects of failures as discussed in Section 5.3.1 of NEI 01-01. The staff made no changes to the RIS based on this comment.

Comment No. 6-16

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.

NRC Response
The NRC staff acknowledges this comment and deleted the associated bullet in Table 1 of the RIS.

Comment No. 6-17

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

NRC Response
The NRC staff agrees with this comment. The staff revised Section 4.1 the RIS and removed the term "implausible" from the document.

Comment No. 6-18

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.

NRC Response
The NRC staff disagrees with this comment. The use of "help to minimize" is accurate because only in some cases is CCF addressed entirely. The staff made no changes to the RIS based on this comment.

Comment No. 6-19

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.

NRC Response
The NRC staff disagrees with this comment. The staff notes that NEI 01-01 references BTP 7-19, Revision 4, rather than Revision 6. The determination of the appropriate engineering criteria to address diversity and defense-in-depth is beyond the scope of the RIS. The staff made no changes to the RIS based on this comment.

Comment No. 6-20

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

NRC Response
The NRC staff disagrees with this comment. The use of the phrase "introduced potential" implies that there may be a new failure. However, the RIS has been revised and these words are no longer in the document. The staff made no changes to the RIS based on this comment.

Comment No. 6-21

*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.*

NRC Response
The NRC staff agrees with this comment. The staff revised Table 2, and it no longer contains the example cited above. However, the staff modified Section 4.1 of the RIS to include the suggested example.

Comment No. 6-22

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.

NRC Response
The NRC staff agrees with the comment. The staff revised Section 3 of the RIS to provide examples of proposed digital I&C modifications that could readily be implemented without prior NRC approval (e.g., modifications to non-safety related systems).

Comment No. 6-23

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.

NRC Response
The NRC staff agrees that the RIS is silent on 10 CFR 50.50(c)(2)(iii). The RIS focuses on the use of qualitative assessments to address 10 CFR 50.59(c)(2), Criteria (i), (ii), (v), and (vi). Guidance on the other 10 CFR 50.59 criteria is beyond the scope of this RIS. The staff made no changes to the RIS based on this comment.

Comment No. 6-24

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.

NRC Response
The NRC staff disagrees with this comment. The discussion in the RIS is consistent with Section 3.2 of NEI 96-07, Revision 1, where the definition of the term "accidents" also includes anticipated operational occurrences. The staff made no changes to the RIS based on this comment.

Letter 7—Comment from Kenneth Scarola

Comment No. 7-1

25. Table 1 – The following design attributes are defined in this table for consideration in the Qualitative Assessment to reach a "sufficiently low" conclusion:

- *Watchdog timers*
- *Segmentation*
- *Self-testing and self-diagnostics*
- *Fail-safe or known to be the same*

These attributes are limiting measures that may contribute to a conclusion that there is not a malfunction with a different result (50.59 Question vi). They are not preventive measures; therefore, they are completely unrelated and have no effect (positive or negative) on malfunction likelihood (i.e., they have no effect on meeting the "sufficiently low" threshold). For example, a

fail-safe design that is more likely to reach that failure state than its analog predecessor yields an unfavorable answer to 50.59 Question ii.

The RIS should be very clear that "sufficiently low" cannot be reached without deterministic design attributes that address the potential for a CCF from every shared resource, including controllers, digital communications, digital HSI and shared digital designs. Here are some examples of preventive measures for various shared resources:

1. *Shared controller – Two controllers running in parallel whose control outputs are continuously compared, such that output state changes are blocked unless the output states from both controllers agree. This prevents a CCF of all functions controlled by that controller, due to a random hardware failure.*
2. *Shared digital data communication network – Communication processors that are separate from function processors. This prevents a CCF of all functions controlled by each controller due to a data storm.*
3. *Shared HSI – Two separate operator actions, with two separate communication messages for all control commands. This prevents a CCF of multiple control functions due to single failure or single design defect that could otherwise generate multiple erroneous commands.*
4. *Shared digital design – Diversity and configuration at the application level to ensure triggered defects are (1) non-concurrent (among multiple devices) and (2) self-announcing in any device where the defect is triggered. This ensures a design defect can be corrected before it is triggered in multiple devices to become a CCF. At this time, this preventive measure is only applicable to non-safety digital upgrades, because until BTP 7-19 is revised only simplicity and diversity can be credited to prevent a CCF due to a design defect.*

NRC Response
The NRC staff agrees with this comment. Sections 3 and 4 of the RIS state, in part, that incorporation of appropriate design attributes can help ensure that a proposed modification does not introduce reductions in redundancy, diversity, separation, or independence of UFSAR-described design functions. The RIS was revised to state that an adequate qualitative assessment of the likelihood of failure of a proposed modification would describe the specific design attributes incorporated to resolve the identified potential failures. The staff made no changes to the RIS based on this comment.

Letter 8—Comments from Tennessee Valley Authority

Comment No. 8-1

Summary of Issue - Page 3 of 5

Tennessee Valley Authority (TVA) agrees with the recommendation from the Nuclear Energy Institute (NEI), and would like to emphasize that this RIS should maintain balanced language regarding the benefits versus risks of digital upgrades, so that licensees will make effective choices to continue the significant safety and reliability benefits that have been realized from digital upgrades, and not be deterred from incorporating digital designs.

NRC Response
The NRC staff agrees with this comment. The staff revised the Summary of Issue section of the RIS to reflect the benefits of digital modifications.

Comment No. 8-2

Attachment, Section 1 - Page 1 of 17

TVA agrees with the recommendation from NEI, and would like to clarify that qualitative assessment and dependability evaluations are not interchangeable terms. Dependability evaluations are evaluations that support the qualitative assessment. Particularly for changes already in process, it should be noted that a qualitative assessment is not necessarily a single document, but may be reflected within several referenced documents or language in the 10 CFR 50.59 evaluation.

NRC Response
The NRC staff agrees with this comment. A qualitative assessment need not be contained in a single document. However, the staff did not consider it necessary to discuss this in the RIS since it is adequately addressed in NEI 01-01.

Comment No. 8-3

Attachment, Section 2.1, Likelihood Thresholds, 10 CFR 50.59(c)(2)(i) - Page 3 of 17

TVA agrees with the recommendation from NEI, and would like to suggest that the steam generator example be replaced with a more applicable example using a digital instrumentation and control (I&C) function.

NRC Response
The NRC staff disagrees with this comment. There is no need to replace the example. The staff made no changes to the RIS based on this comment.

Comment No. 8-4

Attachment, Section 2.1, Likelihood Thresholds, 10 CFR 50.59(c)(2)(ii) - Page 4 of 17

TVA agrees with the recommendation from NEI, and would like to suggest that if the NEI recommendation is not adopted that the "sufficiently low" consideration should be applied only to common cause failure (CCF) probability. For 10 CFR 50.59 question 2, the change must not introduce more than a minimal increase in the malfunction likelihood. Because question 2 is not really about CCF, the "sufficiently low criteria" should not be applied.

NRC Response
The NRC staff disagrees with this comment. "Sufficiently low" may be used to address 10 CFR 50.59(c)(2), Criteria (i), (ii), (v), and (vi). A conclusion of not "sufficiently low" can be evaluated further using the remaining portions of 10 CFR 50.59 criteria (e.g., 10 CFR 50.59(c)(2)(vi) includes two factors—one related to possibility of a malfunction and another to whether that malfunction has a different result than any previously evaluated in the UFSAR). This RIS provides guidance only addressing the threshold of "sufficiently low" needed to support the 10 CFR 50.59 evaluation. The staff made no changes to the RIS based on this comment.

Comment No. 8-5

Attachment, Section 3 - Page 5 of 17

TVA agrees with the recommendation from NEI, and would like to emphasize the need for clarity to avoid aversion to making digital upgrades. If the NEI recommendation is not implemented, this section should specifically clarify:

1) all digital upgrades combine design functions (multi hardware into software design functions) - functions of concern are FSAR design functions
2) "create a CCF vulnerability" as the term is very subjective and requires clarification
3) creating new failure modes is the issue, not combining functions
4) if a potential vulnerability can be mitigated, a qualitative assessment should be acceptable
5) input/output state analysis - provide a reference for this type of testing or clarify. Is this black box, just testing input vs outputs and not internal state testing?

NRC Response
The NRC staff agrees with this comment. The staff revised Section 3 of the RIS to provide examples of proposed digital I&C modifications that could readily be implemented without prior NRC approval (e.g., modifications to non-safety related systems).

Comment No. 8-6

Attachment, Section 3.1.3 - Page 8 of 17

TVA agrees with the recommendation from NEI to replace section 3.1.3, and would like to emphasize that regarding the last paragraph on page 8, the "referenced design" is problematic for operating history. Licensees will often not be able to obtain specific details of the referenced design, for example, when obtaining aggregate failure data from vendors, as specific design features are often related to individually identifiable information that is not publicly shared. Additionally, the reference to "common cause failures" should actually refer to failures in general, not just CCFs.

NRC Response
The NRC staff acknowledges this comment. The level of detailed operating experience available to the licensee will determine the extent to which it can be credited in the qualitative assessment. It is recognized that the level of detail will vary and must be considered on a case by case basis. The staff made no changes to the RIS based on this comment.

Comment No. 8-7

Attachment, Table 1 - Page 9 of 17

TVA agrees with the recommendation from NEI to replace Table 1, and would like to emphasize the importance of clear, precise language to ensure effective application and implementation of qualitative assessments for digital upgrades according to safety function and classification (safety or non-safety related).

NRC Response
The NRC staff agrees with this comment. Staff revised Table 1 of the RIS in a manner

consistent with the theme of the comment. The revisions include the separation of safety-related and non-safety related considerations.

Comment No. 8-8

Attachment, Section 4.2 - Page 11 of 17

TVA agrees with the recommendation from NEI to delete Section 4 in its entirety. If Section 4.2 text is retained, it should acknowledge that using identical software in independent divisions does result in a minuscule reduction of independence. Section 4.2 should provide allowance that if the likelihood of failure is sufficiently low, that minor reduction in independence would not require prior NRC approval.

NRC Response
The NRC staff disagrees with this comment. The staff revised Section 4 of the attachment to the RIS to provide guidance on failure analysis. The staff also revised the title of Section 4 in the RIS to "Engineering Evaluation: Failure Analysis." Identical software on redundant trains/divisions does not affect independence of the redundant trains/divisions provided there is no interconnectivity. The staff made no changes to the RIS based on this comment.

Comment No. 8-9

Attachment, Section 4.3 - Page 11 of 17

TVA agrees with the recommendation from NEI to delete section 4 in its entirety. If Section 4.3 text is retained, the reference to "procedures" should be clarified as to what procedures are being referred to because new procedure coping actions for a CCF would be out of scope of this RIS.

NRC Response
The NRC staff disagrees with this comment. The staff revised Section 4 of the attachment to the RIS to provide guidance on failure analysis. In the revised Section 4, the reference to procedures that can be used to mitigate CCF is clear and does not need further clarification. The staff made no changes to the RIS based on this comment.