## NRR-DMPSPEm Resource

**From:** HANSON, Jerud <jeh@nei.org>
**Sent:** Monday, March 12, 2018 1:54 PM
**To:** Benner, Eric; Govan, Tekia
**Cc:** REMER, Jason; HANSON, Jerud
**Subject:** [External_Sender] Industry Feedback for March 14th RIS Public Meeting
**Attachments:** NEI Members Comment Worksheet - March 2018 RIS Version 3-12-2018.xlsx; ML18051A084 - RIS 2017-XX - With Line Numbers.pdf; RIS Operating Experience Section Suggested Rewrite.pdf; Table 2 Suggested Revision.pdf

Eric/Tekia,

Attached you will find documents detailing comments provided by NEI members on the latest version of the RIS. There are a total of 34 comments for our discussion on Wednesday with the following breakdown:

- Priority 1 (Showstoppers) – 18
- Priority 2 (Important and should be incorporated) – 11
- Priority 3 (Editorial) – 5

For each of the comments, we have provided a suggested rewrite that incorporates our recommendation. In some cases, the proposed rewrite is included in a separate document and attached to this email. Each comment is identified with a line number corresponding to the attached version of the RIS with line numbers added. I recommend we start with the Priority 1 comments, and work our way down the list. The spreadsheet is arranged such that the Priority 1 comments are first, followed by the Priority 2, and then Priority 3. As we work our way through the comments, we will refer to the supplemental attachments provided, which include a suggested rewrite of the operating experience section, as well as Table 2. I think it would also be very helpful if you could provide hard copies during the public meeting.

Please contact me with any questions.

Thank you,

Jerud

**Jerud E. Hanson** | *Sr. Project Manager,*
*Life Extension & New Technology*
1201 F Street, NW, Suite 1100 | Washington, DC 20004
P: 202.739.8053 M: 202.497.2051
nei.org

**Hearing Identifier:** NRR_DMPS
**Email Number:** 244

**Mail Envelope Properties** (1290D5881ECCFA4FBF93A2D70AC229067C7CC765)

**Subject:** [External_Sender] Industry Feedback for March 14th RIS Public Meeting
**Sent Date:** 3/12/2018 1:53:37 PM
**Received Date:** 3/12/2018 1:54:12 PM
**From:** HANSON, Jerud

**Created By:** jeh@nei.org

**Recipients:**
"REMER, Jason" <sjr@nei.org>
Tracking Status: None
"HANSON, Jerud" <jeh@nei.org>
Tracking Status: None
"Benner, Eric" <Eric.Benner@nrc.gov>
Tracking Status: None
"Govan, Tekia" <Tekia.Govan@nrc.gov>
Tracking Status: None

**Post Office:** MBX023-E2-VA-2.EXCH023.DOMAIN.LOCAL

| **Files** | **Size** | **Date & Time** |
|---|---|---|
| MESSAGE | 2614 | 3/12/2018 1:54:12 PM |
| NEI Members Comment Worksheet - March 2018 RIS Version 3-12-2018.xlsx | 28896 | |
| ML18051A084 - RIS 2017-XX - With Line Numbers.pdf | 321831 | |
| RIS Operating Experience Section Suggested Rewrite.pdf | 29849 | |
| Table 2 Suggested Revision.pdf | 64825 | |

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

| INDUSTRY COMMENTS TO MARCH 2018 DRAFT RIS 17-XX SUPPLEMENT-1 TO RIS 2002-22 | | | | | | |
|---|---|---|---|---|---|---|
| **LINE NO.** | **PAGE NO.** | **PRIORITY** | **INDUSTRY COMMENT** | **RECOMMENDED CHANGE** | **ADDITIONAL COMMENTS** | **ACTION TAKEN** |
| 61 | 2 of 5 | 1 | Stating that DI&C upgrades associated with the RPS/ESFAS is 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 significantly limits the SSCs available to be upgraded under this RIS Supplement. | Suggest replacing 2 sentences starting on line 61:<br><br>"This RIS Supplement is not directed toward large-scale analog-to-digital upgrades of the reactor trip and engineered safety features actuation logic, since application of the guidance in this RIS Supplement to such changes would likely involve additional considerations. This RIS Supplement does not provide new design process guidance; however it does highlight vulnerabilities that could be introduced by a digital modification that should be considered in the design process." | | |
| 445 | 4 of 17 | 1 | Section 3: Suggesting revising (or deleting) the wording in Section 3 (Lines 446 to 491).<br><br>The existing wording will be interpreted by licensees such that of a non-safety related DCS would require a LAR to implement. Additionally, item 1.c would prevent a licensee from a simple one-for-one replacement of antiquated analog/pneumatic sequencer timing relays with modern timing relays containing an embedded digital device. Item 3 reintroduces 100% testing which is not possible to achieve 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. | Suggested wording:<br><br>The following examples of proposed changes are considered within the scope of this RIS. The list is by no means inclusive and is simply provided to illustrate the nature and relative complexity of proposed changes targeted by the RIS.<br><br>• A one-for-one replacement of analog timing relays with digital timing relays on redundant load sequencer trains<br>• Replacement of emergency diesel generator (EDG) analog voltage regulators with digital voltage regulators<br>• Replacement of EDG auxiliary support system analog controls with digital controls<br>• Replacement of turbine driven auxiliary feedwater system controls with digital controls<br>• Installation of safety related breakers and relays (including timing relays) containing embedded digital devices<br>• Replacement of safety related analog and electromechanical protective relays with digital multifunction relays<br>• All digital upgrades to non-safety related systems are within the scope of this RIS<br><br>Proposed changes that employ digital equipment with complex application software in redundant safety related trains is considered beyond the scope of this RIS (e.g., a complete analog-to-digital RPS upgrade). Additionally, proposed changes that add new cross-channel communications between redundant safety related trains/equipment would also be considered beyond the scope of this RIS. | | |
| 482 | 5 of 17 | 1 | Section 3, Item 1c) should be deleted from the RIS, as it already excludes RPS and ESFAS. With respect to emergency load sequencers, this is new requirement that was not previously contained in any of the I&C guidance documents. The emergency load sequencers are clearly not part of the RPS or ESFAS. They are within the scope of the onsite AC power system, with guidance contained in SRP Section 8.3. | Remove this section from the RIS. Including the emergency load sequencers would appear to be a backfit issue. | | |
| 485 | 5 of 17 | 1 | Section 3, Item 2: "reduces, redundancy, diversity, separation or independence" - if these attributes are design features, rather than design, or regulatory requirements for that design function, it may not be necessary to maintain that level of UFSAR described redundancy, diversity, separation, or independence to be an acceptable design. In other words, if these are not "credited" then maintaining those design features may not be required. This particularly true for non-safety related systems, where these attributes are not typical required. | Suggest eliminating this section. If it is kept, then suggest clarifying that the impact of reducing these needs to be assessed for the impact on the plant safety analysis. | | |
| 489 | 5 of 17 | 1 | The industry has previously commented on the use of the term "100%" testing, and the terms "simple" or "simplicity". These should be noted as examples of, but not the only examples of, design attributes that can be used in conjunction with other things, such as quality and Operating Experience. | Suggest removing this from this section, and correcting it in the later table in the RIS attachment. Industry and NRC had previously settled on the term "highly testable". For example, a circuit breaker or timing relay with an EDD would be examples of digital devices that are "highly testable". They each have one input and one output and can be easily tested to verify full functionality and repeatability. | | |

| INDUSTRY COMMENTS TO MARCH 2018 DRAFT RIS 17-XX SUPPLEMENT-1 TO RIS 2002-22 | | | | | | |
|---|---|---|---|---|---|---|
| **LINE NO.** | **PAGE NO.** | **PRIORITY** | **INDUSTRY COMMENT** | **RECOMMENDED CHANGE** | **ADDITIONAL COMMENTS** | **ACTION TAKEN** |
| 573 | 7 of 17 | 1 | Section 3.1.2 - Quality of the Design Process: This comment applies to Lines 573 through 590. The two paragraphs discussing industry standards. Licensees will interpret this guidance in a way that concludes non-safety related equipment must comply with industry standards. | Consider replacing the last 3 paragraphs of this section with the following:<br><br>"Quality of the design process is a key element in determining the dependability of SSCs affected by proposed modifications. Licensees employing design processes consistent with their NRC-approved quality assurance programs will result in a quality design process."<br><br>"The use of applicable industry consensus standards contributes to a quality design process and provides a previously established acceptable approach. In some cases, other nuclear or non-nuclear standards also provide technically justifiable approaches that can be used if confirmed applicable for the specific application."<br><br>"For non-safety related SSCs, adherence to generally accepted quality standards is sufficient. The qualitative assessment should list the generally accepted industry standards utilized by the equipment manufacturer. If an equipment manufacturer used NRC-endorsed industry standards during the design and/or manufacturing process for non-safety related equipment, these standards should be documented in the qualitative assessment to provide additional evidence of quality."<br><br>"Specific NRC-endorsed industry standards may be required for qualification of safety related equipment depending on the licensees Appendix B quality assurance program and specific commitments made within their licensing bases. The qualitative assessment should provide evidence that the required industry standards were used in the design as applicable. Any additional industry standards used should also be documented as this can help bolster the quality argument." | | |
| 592 | 7 of 17 | 1 | Section 3.1.3 - Operating Experience - Several issues noted.<br><br>The language seems focused on applicability with specific sited references or evidence:<br>Examples:<br>• Page 8 – 1st para - "…with comparable performance standards and operating environments."<br>• Page 8 – 2nd para - "In all cases, the architecture of the referenced equipment…."<br>• Page 8 - 3rd para - "…what operating conditions were experienced by the reference design."<br><br>At the site inspection level, this type of language would be problematic as it appears 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, so traceability or specific references to environmental conditions and other design attributes are not generally possible to obtain. | Suggestions:<br><br>Be less prescriptive on specific evidence required and focus more on what the value of operating history can provide and define what industry should be looking for such as:<br><br>• Operating history should be viewed as the largest test bed you could ask for. What you want is a large population used across various industries and in a vast range of operating conditions, many different applications, etc. The vendor should have published requirements (e.g., temperature, humidity, voltage limits) for the product. Licensees have an engineering design process that verifies plant environments against these published vendor design specs. This should be left to engineering judgment - the RIS should not require specific environmental evidence as part of the operating history evaluation.<br><br>• Another area to look at is whether the vendor has a corrective action or problem reporting structure, what is their threshold for problem reporting, and is the data used to fix and improved the product. This was touched on in last sentence of page 8, para 1. | See industry provided write-up for the Operating Experience section. | |

| INDUSTRY COMMENTS TO MARCH 2018 DRAFT RIS 17-XX SUPPLEMENT-1 TO RIS 2002-22 | | | | | | |
|---|---|---|---|---|---|---|
| **LINE NO.** | **PAGE NO.** | **PRIORITY** | **INDUSTRY COMMENT** | **RECOMMENDED CHANGE** | **ADDITIONAL COMMENTS** | **ACTION TAKEN** |
| 592 | 7 of 17 | 1 | Section 3.1.3 - Operating Experience (Continued):<br><br>• It is not clear what are we looking for operating experience to do for us?<br><br>o Provide a failure rate number or<br>o Provide us insight into the vendors product and processes<br>o The insights can be a lot better than the calculated failure rates<br><br>Failure rate numbers are normally military spec numbers based upon sub-component failure rates and are normally inflated (i.e., module has a failure rate of 1000 yrs.). We should be looking at real failure rate numbers based upon operating history.<br><br>Applicability in the past has meant documenting a specific software/hardware version. Also, looking at operating history across revision changes is very valuable. It can provide supporting evidence along with identifying weaknesses in the vendor's programs (e.g., SQA, change management and testing). | Additional Suggestions:<br><br>The OE evaluation should not be specifically focused on a failure rate number. Evaluations should look at the number of failures but it should look at the data (the failure report description) for weaknesses.<br>o Review the problem reports (filtering on specific areas of interest such a redundancy helps to manage large amounts of data)<br>o Repetitive failures would point to a weakness in processes<br>o Look for software failure vs hardware failures (hardware may be more of a concern)<br>o Do not limit operating experience to specific revisions (provides insight into the vendor change process)<br>o Problem reporting process (data representative and are reporting thresholds) and what is done with the data (did they fix the issue)<br>• Table 1 - 3rd bullet - User configurable software applications should not be an issue if you have large population set. Operating experience of user configurable devices will get a large number of different and representative configurations to provide valuable insights. | | |
| 628 | 9 of 17 | 1 | Table 1 - Design Attributes:<br><br>Second bullet - with respect to watchdog timers, suggest the changing to the following to clarify: "Watchdog timers that interface with but operate independently of the software"<br><br>Fourth Bullet: Suggest changing simple (i.e., enabling 100 percent testing or comprehensive testing in combination with analysis of likelihood of occurrence of input/output states not tested)" to "(i.e., highly testable)" as stated on Line 334 of the RIS.<br><br>Fifth Bullet: Suggest changing this item to the following: "Assurance that failures in the new equipment either (1) places the affected SSC in a safe state, (2) are equivalent to or bounded by the failure state of the equipment being replaced, or (3) result in a failure state that is inconsequential at the plant level."<br><br>The last version of the RIS had the following Design Attribute: "Unlikely series of events – evaluation of a given digital I&C modification requires postulating multiple independent detected and/or undetected random failures in order to arrive at a state in which a CCF is actually a concern." Industry would like NRC to consider maintaining this Design Attribute. | | | |

| INDUSTRY COMMENTS TO MARCH 2018 DRAFT RIS 17-XX SUPPLEMENT-1 TO RIS 2002-22 | | | | | | |
|---|---|---|---|---|---|---|
| **LINE NO.** | **PAGE NO.** | **PRIORITY** | **INDUSTRY COMMENT** | **RECOMMENDED CHANGE** | **ADDITIONAL COMMENTS** | **ACTION TAKEN** |
| 628 | 9 of 17 | 1 | Table 1 - Quality of the Design Process: Industry would like NRC to consider changing this part of Table 1 to the following:<br><br><u>Safety related equipment</u>:<br>• Compliance with industry software standards as applicable and required by the plant's licensing basis and preferably those consensus standards currently endorsed by the NRC.<br>• For non-NRC endorsed codes and standards, the licensee should provide a documented explanation for why use of the particular non-endorsed software or system standard is acceptable.<br>• Use of Appendix B vendors or use of the commercial grade dedication process based on the guidance provided in EPRI TR-106439.<br>• Demonstrated qualification testing to withstand environmental conditions within which the SSC is credited to perform its design function (e.g., temperature, humidity, seismic, and EMI/RFI susceptibility) as well as not creating unacceptable EMI/RFI emissions.<br><u>Non-safety related equipment</u>:<br>• Adherence to generally accepted quality standards.<br>• Documentation that equipment manufacturer specifications meet or exceed the temperature, humidity, and EMI/RFI emissions and susceptibility requirements levels equal or better than the equipment being replaced. | | | |
| 628 | 9 of 17 | 1 | Table 1 - Operating Experience: Consider updating the portion of Table 1 based on previous comments on Operating Experience. | | | |
| 730 | 12 of 17 | 1 | The statement: "Sources of CCF, could include the introduction of identical software into redundant channels, the use of shared resources; or the use of common hardware and software among systems performing different design functions." implies that a licensee must evaluate every occurrence within the facility where a digital device is being used. This is a new concept for licensees. A licensee does not currently perform an evaluation of the entire plant to determine if a new piece of equipment to be installed as part of a plant modification happens to be used in some other plant system. | Consider deleting Section 4.3, Failure Analysis. Licensees already have procedural design guidance on the development of various types of failure analyses, including Failure Modes and Effects Analyses, Single Failure Analyses, and Software Hazard Analyses, to name a few.<br><br>As an alternate suggestion - consider removing "or the use of common hardware and software among systems performing different design functions". | Section 4.3 - Failure Analyses - is particularly troubling in that it requires a licensee to evaluate every SSC in the plant for each design change to identify if a given digital component was previously installed. Then the licensee is required to perform an evaluation to determine the potential for CCF across SSCs that use a similar digital device. This in and of itself would turn out to be a very difficult research project. For example, assume a licensee desires to install a digital timing relay in a given SSC. Per the guidance, the licensee would have to identify any other place in the plant where that relay was used and then determine if there is a potential for CCF. Or perhaps a licensee desires to replace an analog Rosemount transmitter with a digital Rosemount transmitter in a given system. Per this guidance, the licensee would have to evaluate the thousands of Rosemount digital transmitter installed across the plant to identify if there is a potential for CCF. This is simply not reasonable. In some cases, the research to comply with this portion of the guidance would take longer than the time needed to complete development of the engineering change package needed to implement the change. | |

## INDUSTRY COMMENTS TO MARCH 2018 DRAFT RIS 17-XX SUPPLEMENT-1 TO RIS 2002-22

| LINE NO. | PAGE NO. | PRIORITY | INDUSTRY COMMENT | RECOMMENDED CHANGE | ADDITIONAL COMMENTS | ACTION TAKEN |
|---|---|---|---|---|---|---|
| 807 | 14 of 17 | 1 | Consider deleting Figure 1. This figure leads a licensee to believe that only a Dependability Evaluation is needed. Licensees would prefer to have the RIS provide guidance strictly on Qualitative Assessments for determining equipment/SSC reliability, and then using the Qualitative Assessment to support arguments made in the 50.59 Evaluation. | | | |
| 810 | 15 of 17 | 1 | Table 2 - See industry version of Table 2. | | | |
| NA | NA | 1 | This document provides a lot of guidance on I&C design, in particular, for non-safety related systems. In some cases, the requirements go beyond what is required by the operational quality assurance program used by licensees, and design and licensing bases requirements for non-safety related systems. The RIS should focus on the licensing aspects, not the design aspects of digital upgrades. | Remove design requirements from the RIS. Inclusion of design attributes is useful, and should remain. | Licensees know how to design - they have very detailed and proceduralized guidance along with a quality assurance program. NRC and licensees have not been aligned on adequate documentation of design considerations. The new RIS is supposed to provide licensees with acceptable methods for documenting qualitative assessments for relaying their design thought process in a way that an inspector can understand pertinent design considerations. | |
| 264 | 1 of 17 | 1 | Introduction of the term "Dependability Evaluation" is not beneficial. Industry would like to limit the RIS scope to development of a Qualitative Assessment. Suggest deleting this entire paragraph. | Suggest eliminating the use of Dependability Evaluation throughout the document, including Section 4.5, and provide guidance only on development of Qualitative Assessment guidance as NEI 01-01 appears to use these two terms interchangeably. | To simplify the RIS, consider only providing guidance on development of a qualitative assessment. With the addition of dependability assessments, a licensee will | |
| 280 | 1 of 17 | 1 | Last paragraph of page, second sentence states: "Section 4 of this attachment provides acceptable approaches for engineering evaluations that may be used in performing and documenting a qualitative assessment." Industry would ask the NRC to consider removing the engineering evaluation sections of the RIS as licensees have existing guidance on development of engineering evaluations for digital changes. | | | |
| 470 | 5 of 17 | 1 | "implicitly" - The use of "implicitly modeled, or "implicitly described" in this section and (b) below are much too vague, and cannot be accurately assessed. | Remove "implicitly" described, or provide a regulatory basis for including it. | | |
| 66 | 2 of 5 | 2 | The statement: "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." should be deleted. This RIS Supplement is essentially providing guidance on how to address DI&C CCF through qualitative assessments. As such, this sentence is somewhat contradictory. | Suggest deleting the sentence or provide a reference to the additional NRC guidance documents that address DI&C CCF. | | |
| 132 | 3 of 5 | 2 | This sends an unbalanced message to the public and other stakeholders, implying that digital modifications are adverse to safety. | Replace the first two sentences starting on line 132 with the following:<br><br>"In general, utilization of proven digital technology has the potential for significant improvements in the performance and reliability of equipment used in nuclear plants. Care is appropriate in the implementation of digital technology to avoid unintended consequences that could include potential software failure, including common cause failure, or changes introduced in the transition from analog to digital technology including the scope and effect of a potential failure due to consolidation or reconfiguration of equipment. The potential for these unintended consequences can be appropriately managed in the design process as documented in engineering evaluations and addressed in the assessment of the change required by 10 CFR 50.59 to determine whether NRC approval is required prior to implementation." | | |
| 354 | 3 of 17 | 2 | The following statement is problematic: "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 it is irrelevant to the discussion and is not an accurate statement. Please provide the basis for declaring that the potential for SCCF is directly proportional to the potential increase in likelihood of failure, as not all failures are common cause.<br><br>As an alternative, use the wording suggested for Line 132 above. | 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. | |

## INDUSTRY COMMENTS TO MARCH 2018 DRAFT RIS 17-XX SUPPLEMENT-1 TO RIS 2002-22

| LINE NO. | PAGE NO. | PRIORITY | INDUSTRY COMMENT | RECOMMENDED CHANGE | ADDITIONAL COMMENTS | ACTION TAKEN |
|---|---|---|---|---|---|---|
| 375 | 3 of 17 | 2 | "directly related" - Not all equipment in a system that performs a design function has an equal contribution to the likelihood of malfunction of that design function. It may be directly related, but may not directly increase the likelihood. In other words, the contribution of the I&C potential common cause failure to the overall failure probability of the design function, is not a "one to one" relationship. | This should be clarified here, and in other sections of the document that use this discussion. | | |
| 455 | 5 of 17 | 2 | "vulnerability" - There is not an issue if a CCF vulnerability is created, that is either bounded by existing analyses, or has no safety impact. The key is to assess the vulnerability. | Suggest eliminating this section. If it is kept, then suggest clarifying that the vulnerability needs to be assessed for the impact on the plant safety analysis. | | |
| 701 | | 2 | Combining design functions - This section uses several similar, but very different terms, such as "design functions", "component functions" and "design functions of SSCs". This is confusing. In particular for non-safety related systems, there is no requirement to keep SSCs separate, nor a restriction on combining them. | This section should be simplified to state that if design functions are combined as a result of a digital upgrade, that the vulnerabilities to common cause software failure need to be identified, understood, and analyzed for impact on the plant safety analysis. The rationale should be explained in the engineering documentation or qualitative assessment. | | |
| 775 | 12 of 17 | 2 | "risk significant" - The use of the term “risk significant” needs to be clarified here, and in other places in the document. The context appears to be implying “safety significant”. If that is the case, then the document should tie together this concept by equating risk significant to “important to safety” in technical space. This would better align with the use of “design functions” in 50.59 space. | Define the use of risk significant, or remove it. | | |
| 794 | 13 of 17 | 2 | Section 4.6, Engineering Documentation. Consider deleting this section as licensees already have procedural guidance for development of retainment of the various engineering products required to support a engineering design change in accordance with their Appendix B quality programs. | | | |
| 810 | 15 of 17 | 2 | Table 2 - Step 1, last bullet - the use of "mode" needs to be defined. This could be interpreted that an evaluation of design functions in different plant modes (Mode 1, Mode 2, etc.) is required. | Clarify the use of mode, or delete it. | | |
| 137 | 3 of 5 | 2 | Concern: The RIS expands the use of “qualitative assessment” beyond its use in NEI 01-01. In NEI 01-01, the term is primarily used to address software. Hardware can be assessed deterministically (i.e. not qualitatively, or with engineering judgment). In the RIS, the qualitative assessment is expanded to include deterministic hardware considerations. | Minor changes throughout the document can resolve the consistency issue. | | |

## INDUSTRY COMMENTS TO MARCH 2018 DRAFT RIS 17-XX SUPPLEMENT-1 TO RIS 2002-22

| LINE NO. | PAGE NO. | PRIORITY | INDUSTRY COMMENT | RECOMMENDED CHANGE | ADDITIONAL COMMENTS | ACTION TAKEN |
|---|---|---|---|---|---|---|
| 137 | 3 of 5 | 2 | Concern: The sentence starting with "A qualitative assessment…" on line 137 is an abrupt change that introduces new terminology and concepts without appropriate transition. | Propose that the balance of that paragraph and the following paragraph, lines 137 through 153, be replaced with the following:<br><br>"Conforming changes will follow in the body of the RIS Appropriate considerations in the engineering evaluations can avoid potential unintended consequences of a digital upgrade and provide reasonable assurance that the change results in dependable equipment supporting design functions, including that the software will support the intended design functions. Hardware implemented in the change can be designed to ensure functions are not combined in a manner that expands the impact of a potential failure beyond that evaluated in the plant Final Safety Analysis Report, as updated. Utilization of appropriate software development processes, design attributes, and operating experience can provide assurance that the software will be reliable, with a sufficiently low likelihood of failure.<br><br>"Prior to implementing a digital upgrade, licensees assess the change using the criteria in 10 CFR 50.59 to determine whether the change can be implemented without prior NRC approval. Assessment of the hardware and design configuration considerations can be addressed deterministically. Assessment of the software can be addressed qualitatively to conclude that the likelihood of a consequential software failure is sufficiently low, such that the effects of a software failure, including potential common cause failure, need not be further evaluated. Both hardware and software considerations need to be assessed to support a conclusion that prior NRC approval is not required. The attachment to this RIS supplement provides a framework for preparing and documenting engineering evaluation and qualitative assessments of software." | | |
| 137 | 3 of 5 | 3 | Concern: The sentence starting with "A qualitative assessment…" on line 137 is the start of a new topic and should start a new paragraph. | Start a new paragraph. | **EDITORIAL** | |
| 311 | 2 of 17 | 3 | "Adverse" has a distinct meaning in the 50.59 screening process. The use of adverse in the RIS does line up with the meaning of adverse in 50.59. | Replace "adverse" with "negative' in both places it appears in the document. | **EDITORIAL** | |
| 345 | 2 of 17 | 3 | Suggest deleting the following statement: "This “sufficiently low” threshold is not interchangeable with that for distinguishing between events that are “credible” or “not credible.” 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 UFSAR." | Suggest deleting this statement as it is irrelevant to the discussion and may cause confusion. In addition, the term is not used anywhere else in the document. | **EDITORIAL** | |
| 371 | | 3 | This example uses a steam generator tube rupture event. This does not support use by I&C engineers. | Suggest using an I&C example. | **EDITORIAL** | |
| 527 | 6 of 17 | 3 | 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." | | **EDITORIAL** | |

UNITED STATES
NUCLEAR REGULATORY COMMISSION
OFFICE OF NUCLEAR REACTOR
REGULATION OFFICE OF NEW REACTORS
WASHINGTON, D.C. 20555-0001

Month XX, 2018

**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**

## ADDRESSEES

All holders and applicants for power reactor operating licenses or construction permits under Title 10 of the *Code of Federal Regulations* (10 CFR) Part 50, "Domestic Licensing of Production and Utilization Facilities."

All holders of and applicants for a combined license, standard design approval, or manufacturing license under 10 CFR Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants." All applicants for a standard design certification, including such applicants after initial issuance of a design certification rule.

All holders of, and applicants for, a construction permit or an operating license for non-power production or utilization facilities under 10 CFR Part 50, including all existing non-power reactors and proposed facilities for the production of medical radioisotopes, such as molybdenum-99, except those that have permanently ceased operations and have returned all of their fuel to the U.S. Department of Energy.

## INTENT

The U.S. Nuclear Regulatory Commission (NRC) is issuing a supplement to Regulatory Issue Summary (RIS) 2002-22, dated November 25, 2002 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML023160044). In RIS 2002-22, the NRC staff endorsed "Guideline on Licensing Digital Upgrades: EPRI TR-102348, Revision 1, NEI 01-01: A Revision of EPRI TR-102348 to Reflect Changes to the 10 CFR 50.59 Rule," (Nuclear Energy Institute (NEI) hereinafter "NEI 01-01") (ADAMS Accession No. ML020860169). NEI 01-01 provides guidance for designing, licensing, and implementing digital upgrades and replacements to instrumentation and control (I&C) systems (hereinafter "digital I&C") in a consistent and comprehensive manner.

The purpose of this RIS Supplement is to clarify RIS 2002-22, which remains in effect. The NRC continues to endorse NEI 01-01 as stated in RIS 2002-22, as clarified by this RIS Supplement. Specifically, the guidance in this RIS Supplement clarifies the NRC staff's endorsement of the guidance pertaining to Sections 4, 5, and Appendices A and B of NEI 01-01. This RIS Supplement clarifies the guidance for preparing and documenting "qualitative assessments," that can be used to evaluate the likelihood of failure of a proposed digital modification, including the likelihood of failure due to a common cause, i.e., common cause failure (CCF). Licensees can use these qualitative assessments to support a conclusion that a

proposed digital I&C modification has a sufficiently low[1] likelihood of failure. This conclusion, and the reasons for it, should be documented, per 10 CFR 50.59(d)(1), as part of the evaluations of proposed digital I&C modifications against some of the criteria in 10 CFR 50.59, "Changes, tests and experiments."

This RIS Supplement is not directed toward digital I&C upgrades and replacements of reactor protection systems and engineered safety features actuation systems, since application of the guidance in this RIS Supplement to such changes would likely involve additional considerations. This RIS Supplement does not provide new design process guidance for addressing common cause failure of the reactor protection systems and engineered safety features actuation systems. 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.

This RIS Supplement requires no action or written response on the part of an addressee.

**BACKGROUND INFORMATION**

By letter dated March 15, 2002, NEI submitted EPRI TR-102348, Revision 1 (NEI 01-01) for NRC staff review. NEI 01-01 replaced the original version of EPRI TR-102348, dated December 1993, which the NRC endorsed in Generic Letter 1995-02, "Use of NUMARC/EPRI Report TR-102348, "Guideline on Licensing Digital Upgrades," in Determining the Acceptability of Performing Analog-to-Digital Replacements Under 10 CFR 50.59," dated April 26, 1995 (ADAMS Accession No. ML031070081). In 2002, the NRC staff issued RIS 2002-22 to notify addressees that the NRC staff had reviewed NEI 01-01 and was endorsing the report for use as guidance in designing and implementing digital upgrades to nuclear power plant instrumentation and control systems.

Following the NRC staff's 2002 endorsement of NEI 01-01, holders of construction permits and operating licenses have used that guidance in support of digital design modifications in conjunction with Regulatory Guide 1.187, "Guidance for Implementation of 10 CFR 50.59, Changes, Tests, and Experiments," dated November 2000 (ADAMS Accession No. ML003759710), which endorsed NEI 96-07, "Guidelines for 10 CFR 50.59 Implementation," Revision 1, dated November 2000 (ADAMS Accession No. ML003771157).

NRC inspections of documentation for digital I&C plant modifications prepared by some licensees using the guidance in NEI 01-01 identified inconsistencies in the performance and documentation of licensee engineering evaluations. NRC inspections also identified documentation issues with the written evaluations of the 10 CFR 50.59(c)(2) criteria. The term "engineering evaluation" refers to evaluations performed in designing digital I&C modifications *other* than the 10 CFR 50.59 evaluation, for example, evaluations performed under the licensee's NRC approved quality assurance program. This RIS Supplement clarifies the guidance for licensees performing and documenting engineering evaluations and the development of qualitative assessments.

In response to staff requirements memorandum (SRM)-SECY-16-0070 "Integrated Strategy to Modernize the Nuclear Regulatory Commission's Digital Instrumentation and Control Regulatory

[1] NEI 01-01, Page 4-20, defines "sufficiently low" to mean much lower than the likelihood of failures that are considered in the UFSAR (e.g., single failures) and comparable to other common cause failures that are not considered in the UFSAR (e.g., design flaws, maintenance errors, calibration errors).

Infrastructure (ADAMS Accession No. ML16299A157), NRC staff has engaged the public, including NEI and industry representatives, to improve the guidance for applying 10 CFR 50.59 to digital I&C-related design modifications as part of a broader effort to modernize I&C regulatory infrastructure. Making available the guidance in this RIS Supplement is described as a near-term action in the integrated action plan to provide specific guidance for documenting qualitative assessments concluding that a proposed digital I&C modification will exhibit a sufficiently low likelihood of failure.

Applicability to Non-Power Reactor Licensees

The examples and specific discussion in this RIS Supplement and other guidance referenced by this RIS Supplement (i.e., NEI 01-01 and original RIS 2002-22) primarily focus on power reactors. Nonetheless, licensees of non-power production or utilization facilities (NPUFs) may also use the guidance in RIS 2002-22 and apply the guidance in this RIS Supplement to develop written evaluations addressing the criteria in 10 CFR 50.59(c)(2). In particular, NPUF licensees may use the guidance to prepare qualitative assessments that consider design attributes, quality measures, and applicable operating experience to evaluate proposed digital I&C changes to their facilities as described in Sections 4, 5, and Appendix A of NEI 01-01. However, certain aspects of the guidance that discuss the relationship of other regulatory requirements to 10 CFR 50.59 may not be fully applicable to NPUFs (e.g., 10 CFR Part 50, Appendix A and B are not applicable to NPUFs).

**SUMMARY OF ISSUE**

In general, digital I&C modifications may include a potential for an increase in the likelihood of equipment failures occurring within modified SSCs, including common cause failures. In particular, digital I&C modifications that introduce or modify identical software within independent trains, divisions, or channels within a system, and those that introduce new shared resources, hardware, or software among multiple control functions, may include such a potential. A qualitative assessment can be used to support a conclusion that there is not more than a minimal increase in the frequency of occurrence of accidents or in the likelihood of occurrence of malfunctions (10 CFR 50.59(c)(2)(i) and (ii)). A qualitative assessment can also be used to support a conclusion that the proposed modification does not create the possibility of an accident of a different type or malfunction with a different result than previously evaluated in the UFSAR (10 CFR 50.59(c)(2)(v) and (vi)).

For digital I&C modifications, an adequate basis for a determination that a change involves a sufficiently low likelihood of failure may be derived from a qualitative assessment of factors involving system design features, the quality of the design processes employed, and an evaluation of relevant operating experience of the software and hardware used (i.e., product maturity and in-service experience). A licensee may use a qualitative assessment to document the factors and rationale for concluding that there is an adequate basis for determining that a digital I&C modification will exhibit a sufficiently low likelihood of failure. In doing so, a licensee may consider the aggregate of these factors. The attachment to this RIS Supplement provides a framework for preparing and documenting qualitative assessments and engineering evaluations.

In addition, this RIS Supplement clarifies the applicability of some aspects of the NRC policy described in Item II.Q of SRM/SECY 93-087, Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light Water Reactor (ALWR) Designs, (ADAMS

No. ML003708056), in regard to the application of 10 CFR 50.59(c)(2) criteria for digital I&C modifications.

## BACKFITTING AND ISSUE FINALITY DISCUSSION

This RIS Supplement clarifies but does not supersede RIS 2002-22, and includes additional guidance regarding how to perform and document qualitative assessments for digital I&C changes under 10 CFR 50.59.

The NRC does not intend or approve any imposition of the guidance in this RIS Supplement, and this RIS Supplement does not contain new or changed requirements or staff positions that constitute either backfitting under the definition of backfitting in 10 CFR 50.109(a)(1) or a violation of issue finality under any of the issue finality provisions in 10 CFR Part 52. Therefore, this RIS Supplement does not represent backfitting as defined in 10 CFR 50.109(a)(1), nor is it otherwise inconsistent with any issue finality provision in 10 CFR Part 52. Consequently, the NRC staff did not perform a backfit analysis for this RIS Supplement or further address the issue finality criteria in 10 CFR Part 52.

## FEDERAL REGISTER NOTIFICATION

The NRC will publish a notice of opportunity for public comment on this draft RIS in the *Federal Register*.

## CONGRESSIONAL REVIEW ACT

This RIS is a rule as defined in the Congressional Review Act (5 U.S.C. §§ 801-808). However, the Office of Management and Budget has not found it to be a major rule as defined in the Congressional Review Act.

## PAPERWORK REDUCTION ACT STATEMENT

This RIS provides guidance for implementing mandatory information collections covered by 10 CFR Part 50 that are subject to the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et. seq.). This information collection was approved by the Office of Management and Budget (OMB) under control number 3150-0011. Send comments regarding this information collection to the Information Services Branch, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001, or by e-mail to Infocollects.Resource@nrc.gov, and to the Desk Officer, Office of Information and Regulatory Affairs, NEOB-10202, (3150-0011) Office of Management and Budget, Washington, DC 20503.

### Public Protection Notification

The NRC may not conduct or sponsor, and a person is not required to respond to, a request for information or an information collection requirement unless the requesting document displays a currently valid OMB control number.

**CONTACT**

Please direct any questions about this matter to the technical contact(s) or the Lead Project Manager listed below.

Timothy J. McGinty, Director
Division of Construction Inspection
and Operation Programs
Office of New Reactors

Christopher G. Miller, Director
Division of Inspection and Regional Support
Office of Nuclear Reactor Regulation

Technical Contacts: David Rahn, NRR
301-415-1315
e-mail: David.Rahn@nrc.gov

Wendell Morton, NRR
301-415-1658
e-mail: Wendell.Morton@nrc.gov

Norbert Carte, NRR
301-415-5890
e-mail: Norbert.Carte@nrc.gov

David Beaulieu, NRR
301-415-3243
e-mail: David.Beaulieu@nrc.gov

Duane Hardesty,
NRR 301-415-3724
email: Duane.Hardesty@nrc.gov (Specifically for non-power reactors)

Project Manager Contact: Tekia Govan, NRR
301-415-6197
e-mail: Tekia.Govan@nrc.gov

Note: NRC generic communications may be found on the NRC public Web site, http://www.nrc.gov, under NRC Library/Document Collections.

Attachment: Qualitative Assessment and Engineering Evaluation Framework

## Qualitative Assessment and Engineering Evaluation Framework

### 1. Purpose

Regulatory Issue Summary (RIS) 2002-22 provided the U.S. Nuclear Regulatory Commission (NRC) staff's endorsement of Nuclear Energy Institute (NEI) Guidance document NEI 01-01, "Guideline on Licensing Digital Upgrades: EPRI TR-102348, Revision 1, NEI 01-01: A Revision of EPRI TR-102348 To Reflect Changes to the 10 CFR 50.59 Rule." NEI 01-01 provides guidance for implementing and licensing digital upgrades, in a consistent, comprehensive, and predictable manner, as well as guidance in performing qualitative assessments of the dependability of digital instrumentation and control (I&C) systems.

The purpose of this attachment is to provide supplemental clarifying guidance to licensees to ensure that, if qualitative assessments are used, they are described and documented consistently, through an evaluation of applicable qualitative evidence. Following the guidance in RIS 2002-22 and NEI 01-01, as clarified by the guidance in this RIS Supplement, will help licensees document qualitative assessments "in sufficient detail " that an independent third party can verify the judgements," as stated in NEI 01-01. While this qualitative assessment is used to support the Title 10 of the *Code of Federal Regulations* (10 CFR) 50.59, "Changes tests and experiments," evaluation, it does not provide guidance for screening and it does not presume that all digital modifications "screen in."

NEI 01-01 uses the terms "qualitative assessment" and "dependability evaluations" interchangeably. Within this document only the terms "qualitative assessment" and "sufficiently low[2]" are used in conjunction with performance of 10 CFR 50.59 evaluations. The term "dependability evaluation" is used in the context of engineering evaluations, which are not performed or documented as part of a 10 CFR 50.59 evaluation, but engineering evaluations are performed in accordance with the licensee's NRC quality assurance program in developing digital I&C modification.

If a "qualitative assessment" determines that a potential failure (e.g., software common cause failure (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. In some cases, the effects of a software CCF may not create a different result than any previously evaluated in the updated final safety analysis report (UFSAR).

Sections 2 and 3 of this attachment provide acceptable approaches for describing the scope, form, and content of the type of a qualitative assessment described above. Section 4 of this attachment provides acceptable approaches for engineering evaluations that may be used in performing and documenting a qualitative assessment.

[2] NEI 01-01, Page 4-20, defines "sufficiently low" to mean much lower than the likelihood of failures that are considered in the UFSAR (e.g., single failures) and comparable to other common cause failures that are not considered in the UFSAR (e.g., design flaws, maintenance errors, calibration errors).

## 2. Regulatory Clarification Application of Qualitative Assessments to Title 10 of the *Code of Federal Regulations,* Section 50.59

When a licensee decides to undertake an activity that changes its facility as described in the updated final safety evaluation report, the licensee first performs the engineering and technical evaluations in accordance with plant procedures. If the licensee determines that an activity is acceptable through appropriate engineering and technical evaluations, the licensee enters the 10 CFR 50.59 process. The regulations in 10 CFR 50.59 provide a threshold for regulatory review, not a determination of safety, for the proposed activities. In addition, 10 CFR 50.59 establishes the conditions under which licensees may make changes to the facility or procedures and conduct tests or experiments without prior NRC approval.

Evaluations must address all elements of proposed changes. Some elements of a change may have positive effects on SSC failure likelihood while other elements of a change may have adverse effects. As derived from the guidance in NEI 96-07, positive and negative elements can be considered together if they are interdependent. This means that if elements are not interdependent, they must be evaluated separately.

### 2.1 Likelihood

Properly documented qualitative assessments may be used to support a conclusion that a proposed digital I&C modification has a sufficiently low likelihood of failure, consistent with the UFSAR analysis assumptions. This conclusion is used in the 10 CFR 50.59 written evaluation to determine whether prior NRC approval is required.

Qualitative Assessment

The determination that a digital I&C modification will exhibit a sufficiently low likelihood of failure can be derived from a qualitative assessment of factors involving system design attributes, the quality of the design processes employed, the operating experience with the software and hardware used (i.e., product maturity and in-service experience). Documenting the qualitative assessment includes describing the factors, rationale, and reasoning (including engineering judgement) for determining that the digital I&C modification exhibits a sufficiently low likelihood of failure.

The determination of likelihood of failure may consider the aggregate of all the factors described above. Some of these factors may compensate for weaknesses in other areas. For example, for a digital device that is simple and highly testable, thorough testing may provide additional assurance of a sufficiently low likelihood of failure that helps compensate for a lack of operating experience.

Qualitative Assessment Outcome

There are two possible outcomes of the qualitative assessment: (1) failure likelihood is "sufficiently low," and (2) failure likelihood is not "sufficiently low." Guidance in NEI 01-01, Section 4.3.6, states, "sufficiently low" means much lower than the likelihood of failures that are considered in the UFSAR (e.g., single failures) and comparable to other common cause failures that are not considered in the UFSAR (e.g., design flaws, maintenance error, calibration errors). This "sufficiently low" threshold is not interchangeable with that for distinguishing between events that are "credible" or "not credible." 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 UFSAR.

**Likelihood Thresholds for 10 CFR 50.59(c)(2)(i), (ii), (v), and (vi)**

A key element of 10 CFR 50.59 evaluations is demonstrating whether the modification considered will exhibit a sufficiently low likelihood of failure. For digital modifications, particularly those that introduce software, there may be a potential increase in likelihood of failure. For redundant SSCs, this potential increase in the likelihood of failure creates a similar increase in the likelihood of a common cause failure.

The "sufficiently low" threshold discussions have been developed using criteria from NEI 96-07, Revision 1, and NEI 01-01. They are intended to clarify the existing 10 CFR 50.59 guidance and should not be interpreted as a new or modified NRC position.

Criteria

Although it may be required by other criteria, prior NRC approval is not required by 10 CFR 50.59(c)(2)(i), (ii), (v), and (vi) if there is a qualitative assessment outcome of sufficiently low, as described below:

10 CFR 50.59(c)(2)(i)

Does the activity result in more than a minimal increase in the frequency of occurrence of an accident previously evaluated in the UFSAR?

> "Sufficiently low" threshold — The frequency of occurrence of an accident is directly related to the likelihood of failure of equipment that initiates the accident (e.g., an increase in the likelihood of a steam generator tube failure has a corresponding increase in the frequency of a steam generator tube rupture accident). Thus, an increase in likelihood of failure of the modified equipment results in an increase in the frequency of the accident. Therefore, if the qualitative assessment outcome is "sufficiently low," then there is a no more than a minimal increase in the frequency of occurrence of an accident previously evaluated in the UFSAR.

10 CFR 50.59(c)(2)(ii)

Does the activity 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[3] previously evaluated in the UFSAR?

> "Sufficiently low" threshold — The likelihood of occurrence of a malfunction of an SSC important to safety is directly related to the likelihood of failure of equipment that causes a failure of SSCs to perform their intended design functions[4] (e.g., an increase in the

[3] NEI 96-07, Revision 1, Section 3.9, states, "Malfunction of SSCs important to safety means the failure of SSCs to perform their intended design functions described in the UFSAR (whether or not classified as safety-related in accordance with 10 CFR [Part] 50, Appendix B)."

[4] The term "design functions," as used in this RIS Supplement, conforms to the definition of "design functions" in NEI 96-07, Revision 1.

likelihood of failure of an auxiliary feedwater (AFW) pump has a corresponding increase in the likelihood of occurrence of a malfunction of SSCs the AFW pump and AFW system). Thus, the likelihood of failure of modified equipment that causes the failure of SSCs to perform their intended design functions is directly related to the likelihood of occurrence of a malfunction of an SSC important to safety. Therefore, if the qualitative assessment outcome is sufficiently low, then the activity does not result in more than a minimal increase in the likelihood of occurrence of a malfunction of an SSC important to safety previously evaluated in the UFSAR.

10 CFR 50.59(c)(2)(v)

Does the activity create a possibility for an accident of a different type than any previously evaluated in the UFSAR?

Sufficiently low threshold NEI 96-07, Revision 1, Section 4.3.5, states, Accidents of a different type are limited to those that are as likely to happen as those previously evaluated in the UFSAR. Accidents of a different type are caused by failures of equipment that initiate an accident of a different type. If the outcome of the qualitative assessment of the proposed change is that the likelihood of failure associated with the proposed activity is sufficiently low, then there are no failures introduced by the activity that are as likely to happen as those in the UFSAR that can initiate an accident of a different type. Therefore, the activity does not create a possibility for an accident of a different type than any previously evaluated in the UFSAR. If the qualitative assessment determines that a potential failure (e.g., software CCF) does not have a sufficiently low likelihood, then the effects of this failure need to be considered in the 10 CFR 50.59 evaluation.

10 CFR 50.59(c)(2)(vi)

Does the activity create a possibility for a malfunction of an SSC important to safety with a different result than any previously evaluated in the UFSAR?

Sufficiently low threshold 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. A malfunction of an SSC important to safety is an equipment failure that causes the failure of SSCs to perform their intended design functions. If the outcome of the qualitative assessment of the proposed change is that the likelihood of failure associated with the proposed activity is sufficiently low, then there are no failures introduced by the activity that are as likely to happen as those in the UFSAR. Therefore, the activity does not create a possibility for a malfunction of an SSC important to safety with a different result than any previously evaluated in the UFSAR. If the qualitative assessment determines that a potential failure (e.g., software CCF) does not have a sufficiently low likelihood, then the effects of this failure need to be considered in the 10 CFR 50.59 evaluation using methods consistent with the plants UFSAR.

**3. Qualitative Assessments**

The NRC staff has determined that proposed digital I&C modifications having the characteristics listed below are likely to result in qualitative assessment outcomes that support a sufficiently low likelihood determination:

1. Digital I&C modifications that:

    a) Do not create a CCF vulnerability due to the integration of subsystems or components from different systems that combine design functions that were not previously combined within the same system, subsystem, or component being replaced.

    Note: "Integration," as used in this RIS supplement refers to the process of combining software components, hardware components, or both into an overall system, or the merger of the design function of two or more systems or components into a functioning, unified system or component. Integration also refers to the coupling of design functions (software/ hardware) via bi-directional digital communications. Modifications can result in design functions of different systems being integrated or combined either directly in the same digital device or indirectly via shared resources, such as bi-directional digital communications or networks, common controllers, power supplies, or visual display units. Such integration could be problematic because the safety analysis may have explicitly or implicitly modeled the equipment performing the design functions that would be integrated on the basis that it is not subject to any potential source of common cause failure.

    b) Do not create a CCF vulnerability due to new shared resources (such as power supplies, controllers, and human-machine interfaces) with other design functions that are (i) explicitly or implicitly described in the UFSAR as functioning independently from other plant design functions, or (ii) modeled in the current design basis to be functioning independently from other plant design functions.

    c) Do not affect reactor trip or engineered safety feature initiation/control logic or emergency power bus load sequencers.

2. Digital I&C modifications that maintain the level of diversity, separation, and independence of design functions described in the UFSAR. A change that reduces redundancy, diversity, separation or independence of USFAR-described design functions is considered a more than minimal increase in the likelihood of malfunction.

3. Digital I&C modifications that are sufficiently simple (as demonstrated through 100 percent testing or a combination of testing and input/output state analysis); or demonstrate adequate internal diversity.

**3.1 Qualitative Assessment Categories**

Consistent with the guidance provided in NEI 01-01, this attachment specifies three general categories of characteristics: design attributes, quality of the design process, and operating experience. Qualitatively assessing and then documenting these characteristics separately, by category, and in the aggregate provides a common framework that will better enable licensees

to document qualitative assessments "in sufficient detail" that an independent third party can verify the judgements.

Table 1 provides acceptable examples of design attributes, quality of the design processes, and documentation of operating experience. This listing is not all inclusive nor does the qualitative assessment need to address each specific item.

### 3.1.1 Design attributes

NEI 01-01 Section 5.3.1 states:

> To determine whether a digital system is sufficiently dependable, and therefore that the likelihood of failure is sufficiently low, there are some important characteristics that should be evaluated. These characteristics, discussed in more detail in the following sections include: Hardware and software design features that contribute to high dependability (See Section 5.3.4). Such [hardware and software design] features include built-in fault detection and failure management schemes, internal redundancy and diagnostics, and use of software and hardware architectures designed to minimize failure consequences and facilitate problem diagnosis.

Consistent with the above-quoted text, design attributes of a proposed modification can prevent or limit failures from occurring. A qualitative assessment describes and documents hardware and software design features that contribute to high dependability. Design attributes focus primarily on built-in features such as fault detection and failure management schemes, internal redundancy and diagnostics, and use of software and hardware architectures and facilitate problem diagnosis. However, design features external to the proposed modification (e.g., mechanical stops on valves) may also need to be considered.

Many system design attributes, procedures, and practices can contribute to significantly reducing the likelihood of failure (e.g., CCF). A licensee can account for this by deterministically assessing the specific vulnerabilities through postulated failure modes (e.g., software CCF) within a proposed modification and applying specific design attributes to address those vulnerabilities (see Table 1). An adequate qualitative assessment regarding the likelihood of failure of a proposed modification would consist of a description of: (a) the potential failures introduced by the proposed modification, (b) the design attributes used to resolve identified potential failures, and (c) how the chosen design attributes and features resolve identified potential failures.

Diversity is one example of a design attribute that can be used to demonstrate an SSC modified with digital technology is protected from a loss of design function due to a potential common cause failure. In some cases, a plant's design basis may specify diversity as part of the design. In all other cases, the licensees need not consider the use of diversity (e.g., as described in the staff requirements memorandum on SECY 93-087) in evaluating a proposed modification. However, diversity within the proposed design, and any affected SSCs is a powerful means for significantly reducing the occurrence of failures affecting the accomplishment of design functions.

### 3.1.2 Quality of the Design Process

Section 5.3.3 of NEI 01-01 states:

> For digital equipment incorporating software, it is well recognized that prerequisites for quality and dependability are experienced software engineering professionals combined with well-defined processes for project management, software design, development, implementation, verification, validation, software safety analysis, change control, and configuration control.

Consistent with the guidance provided in NEI 01-01, "Quality Design Processes" means those processes employed in the development of the proposed modification. Such processes include software development, hardware and software integration processes, hardware design, and validation and testing processes that have been incorporated into the development process. For safety-related equipment this development process would be documented and available for referencing in the qualitative assessment for proposed modifications. However, for commercial-grade-dedicated or non-safety related equipment documentation of the development process may not be readily available. In such cases, the qualitative assessment may place greater emphasis on the design attributes included and the extent of successful operating experience for the equipment proposed.

Quality of the design process is a key element in determining the dependability of proposed modifications. Licensees employing design processes consistent with their NRC-approved quality assurance programs will result in a quality design process.

When possible, the use of applicable industry consensus standards contributes to a quality design process and provides a previously established acceptable approach (e.g., Institute of Electrical and Electronics Engineers (IEEE) Standard 1074-2006, "IEEE Standard for Developing a Software Project Life Cycle Process," endorsed in Regulatory Guide 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plant"). In some cases, other nuclear or non-nuclear standards also provide technically justifiable approaches that can be used if confirmed applicable for the specific application.

Quality standards should not be confused with quality assurance programs or procedures. Quality standards are those standards which describe the benchmarks that are specified to be achieved in a design. Quality standards should be documents that are established by consensus and approved by an accredited standards development organization. For example, IEEE publishes consensus-based quality standards relevant to digital I&C modifications and is a recognized standards development organization. Quality standards used to ensure the proposed change has been developed using a quality design process do not need to be solely those endorsed by the NRC staff. The qualitative assessment document should demonstrate that the standard being applied is valid for the circumstances for which it is being used.

### 3.1.3 Operating Experience

Section 5.3.1 of NEI 01-01 states, "Substantial applicable operating history reduces uncertainty in demonstrating adequate dependability."

Consistent with the above-quoted text, relevant operating experience can be used to help demonstrate that software and hardware employed in a proposed modification have adequate dependability. The licensee may document information showing that the proposed system or component modification employs equipment with significant operating experience in nuclear power plant applications, or in non-nuclear applications with comparable performance standards and operating environment. The licensee may also consider whether the suppliers of such equipment incorporate quality processes such as continual process improvement, incorporation of lessons learned, etc., and document how that information demonstrates adequate equipment dependability.

Operating experience relevant to a proposed digital I&C change may be credited as part of an adequate basis for a determination that the proposed change does not result in more than a minimal increase in the frequency of occurrence of initiating events that can lead to accidents or in more than a minimal increase in the likelihood of occurrence of a malfunction of an SSC important to safety previously evaluated in the UFSAR. Differences may exist in the specific digital I&C application between the proposed digital I&C modification and that of the equipment and software whose operating experience is being credited. In all cases, however, the architecture of the referenced equipment and software should be substantially similar to that of the system being proposed.

Further, the design conditions and modes of operation of the equipment whose operating experience is being referenced also needs to be substantially similar to that being proposed as a digital I&C modification. For example, one needs to understand what operating conditions (e.g., ambient environment, continuous duty, etc.) were experienced by the referenced design. In addition, it is important to recognize that when crediting operating experience from other facilities, one needs to understand what design features were present in the design whose operating experience is being credited. Design features that serve to prevent or limit possible common cause failures in a design referenced as relevant operating experience should be noted and considered for inclusion in the proposed design. Doing so would provide additional support for a determination that the dependability of the proposed design will be similar to the referenced application.

628

**Table 1 Qualitative Assessment Category Examples**

| Categories | Examples for Each Category |
|---|---|
| Design Attributes | • Design criteria Diversity (if applicable), Independence, and Redundancy.<br>• Inherent design features for software, hardware or architectural/network Watchdog timers that operate independent of software, isolation devices, segmentation of distributed networks, self-testing, and self-diagnostic features.<br>• Basis for identifying that possible triggers are non-concurrent.<br>• Sufficiently simple (i.e., enabling 100 percent testing or comprehensive testing in combination with analysis of likelihood of occurrence of input/output states not tested).<br>• Failure state always known to be safe, or at least the same state as allowed by the previously installed equipment safety analysis. |
| Quality of the Design Process | • Justification for use of industry consensus standards for codes and standards not endorsed by the NRC.<br>• Justification for use of other standards.<br>• Use of Appendix B vendors. If not an Appendix B vendor, the analysis can state which generally accepted industrial quality program was applied.<br>• Use of Commercial Grade Dedication processes per guidance of EPRI TR-106439, Annex D of IEEE 7-4.3.2, and examples within EPRI TR-107330.<br>• Demonstrated capability (e.g., through qualification testing) to withstand environmental conditions within which the SSC is credited to perform its design function (e.g., EMI/RFI, Seismic).<br>• Development process rigor (adherence to generally-accepted commercial or nuclear standards.)<br>• Demonstrated dependability of custom software code for application software through extensive evaluation or testing. |
| Operating Experience | • Wide range of operating experience in similar applications, operating environments, duty cycles, loading, comparable configurations, etc., to that of the proposed modification.<br>• History of lessons learned from field experience addressed in the design.<br>• Relevant operating experience: Architecture of the referenced equipment and software (operating system and application) along with the design conditions and modes of operation of the equipment should be substantially similar to those of the system being proposed as a digital I&C modification. High volume production usage in different applications Note that for software, the concern is centered on lower volume, custom, or user-configurable software applications. High volume, high quality commercial products with relevant operating experience used in other applications have the potential to avoid design errors.<br>• Experience working with software development tools used to create configuration files. |

### 3.2 Qualitative Assessment Documentation

The U.S. Nuclear Regulatory Commission endorsed guidance for documenting 10 CFR 50.59 evaluations to meet the requirements of 10 CFR 50.59 (d) is provided in both NEI 96-07, Revision 1 in Section 5.0, "Documentation and Reporting" and NEI 01-01, Appendix B. Both of these documents reiterate the principles that documentation should include an "explanation providing adequate basis for the conclusion" so that a "knowledgeable reviewer could draw the same conclusion."

Considerations and conclusions reached while performing qualitative assessments supporting the evaluation criteria of 10 CFR 50.59, are subject to the aforementioned principles. In order for a knowledgeable reviewer to draw the same conclusion regarding qualitative assessments, details of the considerations made, and their separate and aggregate effect on any qualitative assessments need to be included or clearly referenced in the 10 CFR 50.59 evaluation documentation. References to other documents should include the document name and location of the information within any referenced document.

If qualitative assessment categories are used, each category would be discussed in the documentation including positive and negative aspects considered, consistent with the examples provided in Table 1. In addition, a discussion of the degree to which each of the categories was relied on to reach the qualitative assessment conclusion would be documented.

## 4. Engineering Evaluations

### 4.1 Overview

This section describes approaches that could be used for conducting and documenting engineering evaluations. completed in accordance with the licensee's NRC approved quality assurance program. The term "engineering evaluation" refers to evaluations performed in designing digital I&C modifications. These evaluations are performed under the licensee's NRC approved quality assurance program. These engineering evaluations may include, but are not limited to discussion of compliance with regulatory requirements and conformity to the UFSAR, regulatory guidance, and design standards.

In addition, these engineering evaluations may include discussions of: a) the performance of deterministic failure analyses, including analysis of the effects of digital I&C failures at the component-level, system-level, and plant-level; b) the evaluation of defense-in-depth; and c) the evaluation of the proposed modification for its overall "dependability." The qualitative assessment framework discussed in the previous sections of this attachment may rely, in part, on the technical bases and conclusions documented within these engineering evaluations. Thus, improved performance and documentation of engineering evaluations can enable better qualitative assessments.

One result of performing these evaluations is to provide insights as to whether a proposed digital I&C design modification may need to be enhanced with the inclusion of different or additional design attributes. Such different or additional design attributes would serve to prevent the occurrence of a possible CCF or reduce the potential for a software CCF to cause a loss of design function.

These approaches are provided for consideration only. They do not represent NRC requirements and may be used at the discretion of licensees.

### 4.2 Selected Design Considerations

During the design process, it is important to consider both the positive effects of installing the digital equipment (e.g., elimination of single-point vulnerabilities (SPVs), ability to perform signal validation, diagnostic capabilities) with the potential negative effects (e.g., software CCF).

Digital I&C modifications can reduce SSC independence. Reduction in independence of design functions from that described in the USFAR would require prior NRC approval.

#### 4.2.1 Digital Communications

Careful consideration of digital communications is needed to preclude adverse effects on SSC independence. DI&C-ISG-04, Revision 1, "Highly-Integrated Control Rooms - Communications Issues" (Agencywide Documents Access and Management System Accession Number ML083310185) provides guidance for NRC staff reviewing digital communications. This ISG describes considerations for the design of communications between redundant SSCs, echelons of defense-in-depth[5] or SSCs with different safety classifications. The principles of this ISG or other technically justifiable considerations, may be used to assess non-safety related SSCs.

#### 4.2.2 Combining Design Functions

Combining design functions of different safety-related or non-safety related SSCs in a manner not previously evaluated or described in the UFSAR could introduce new interdependencies and interactions that make it more difficult to account for new potential failure modes. Failure of combined design functions that: 1) can effect malfunctions of SSCs or accidents evaluated in the UFSAR; or 2) involve different defense-in-depth echelons; are of significant concern.

Combining previously separate component functions can result in more dependable system performance due to the tightly coupled nature of the components and a reduction in complexity. If a licensee proposes to combine previously separate design functions in a safety-related and/or non-safety related digital I&C modification, possible new failures need to be carefully weighed with respect to the benefits of combining the previous separately controlled functions. Failure analyses and control system segmentation analyses can help identify potential issues. Segmentation analyses are particularly helpful for the evaluation of the design of non-safety related distributed networks.

### 4.3 Failure Analyses

Failure analysis can be used to identify possible CCFs in order to assess the need to further modify the design. In some cases, potential failures maybe excluded from consideration if the failure has been determined to be implausible as a result of factors such as design features/attributes, and procedures. Modifications that employ design attributes and features,

[5] As stated in NEI 01-01, Section 5.2, "A fundamental concept in the regulatory requirements and expectations for instrumentation and control systems in nuclear power plants is the use of four echelons of defense-in-depth: 1) Control Systems; 2) Reactor Trip System (RTS) and Anticipated Transient without SCRAM (ATWS); 3) Engineered Safety Features Actuation System (ESFAS); and 4) Monitoring and indications."

such as internal diversity, help to minimize the potential for CCFs. Sources of CCF, could include the introduction of identical software into redundant channels, the use of shared resources; or the use of common hardware and software among systems performing different design functions. Therefore, it is essential that such sources of CCF be identified, to the extent practicable, and addressed during the design stage as one acceptable method to support the technical basis for the proposed modification.

Digital designs having sources of CCF that could affect more than one SSC need to be closely reviewed to ensure that an accident of a different type from those previously evaluated in the UFSAR has not been created. This is particularly the case when such common sources of CCF also are subject to common triggers. For example, the interface of the modified SSCs with other SSCs using identical hardware and software, power supplies, human-machine interfaces, needs to be closely reviewed to ensure that possible common triggers have been addressed.

A software CCF may be assessed using best-estimate methods and realistic assumptions. Unless already incorporated into the licensee's UFSAR, "best-estimate" methods cannot be used for evaluating different results than those previously evaluated in the UFSAR.

### 4.4 Defense-in-Depth Analyses

NEI 01-01 describes the need for defense-in-depth analysis as limited to substantial digital replacements of reactor protection system and ESFAS. A defense-in-depth analysis for complex digital modifications of systems other than protection systems may also reveal the impact of any new potential CCFs due to the introduction of shared resources, common hardware and software, or the combination of design functions of systems that were previously considered to be independent of one another. Additionally, defense-in-depth analysis may reveal direct or indirect impacts on interfaces with existing plant SSCs. This type of analysis may show that existing SSCs and/or procedures could serve to mitigate effects of possible CCFs introduced through the proposed modification.

### 4.5 Dependability Evaluation

Section 5.3.1 of NEI 01-01 states that a digital system that is sufficiently dependable will have a likelihood of failure that is sufficiently low. This section describes considerations that can be used to determine whether a digital system is "sufficiently dependable."

The dependability evaluation relies on some degree of engineering judgment to support a conclusion that the digital modification is considered to be "sufficiently dependable." When performing a dependability evaluation, one acceptable method is to consider: (1) inclusion of any deterministically-applied defensive design features and attributes; (2) conformance with applicable standards regarding quality of the design process for software and hardware; and (3) relevant operating experience. Although not stated in NEI 01-01, judgments regarding the quality of the design process and operating experience may supplement, but not replace the inclusion of design features and attributes.

For proposed designs that are more complex or more risk significant, the inclusion of design features and attributes that: serve to prevent CCF, significantly reduce the possible occurrence of software CCF, or significantly limit the consequences of such software CCF, should be key considerations for supporting a "sufficiently dependable" determination. Design features

maximizing reliable system performance, to the extent practicable, can also be critical in establishing a basis for the dependability of complex or risk significant designs.

Section 5.1.3 of NEI 01-01 states that "Judgments regarding dependability, likelihood of failures, and significance of identified potential failures should be documented" ." Depending on the SSCs being modified and the complexity of the proposed modification, it may be challenging to demonstrate "sufficient dependability" based solely upon the quality of the design process and/or operating history. Engineering judgments regarding the quality of the design process and operating experience may supplement, but not replace the inclusion of design features and attributes when considering complex modifications.

Figure 1 of this attachment provides a simplified illustration of the engineering evaluations process described in Section 4 of this attachment.

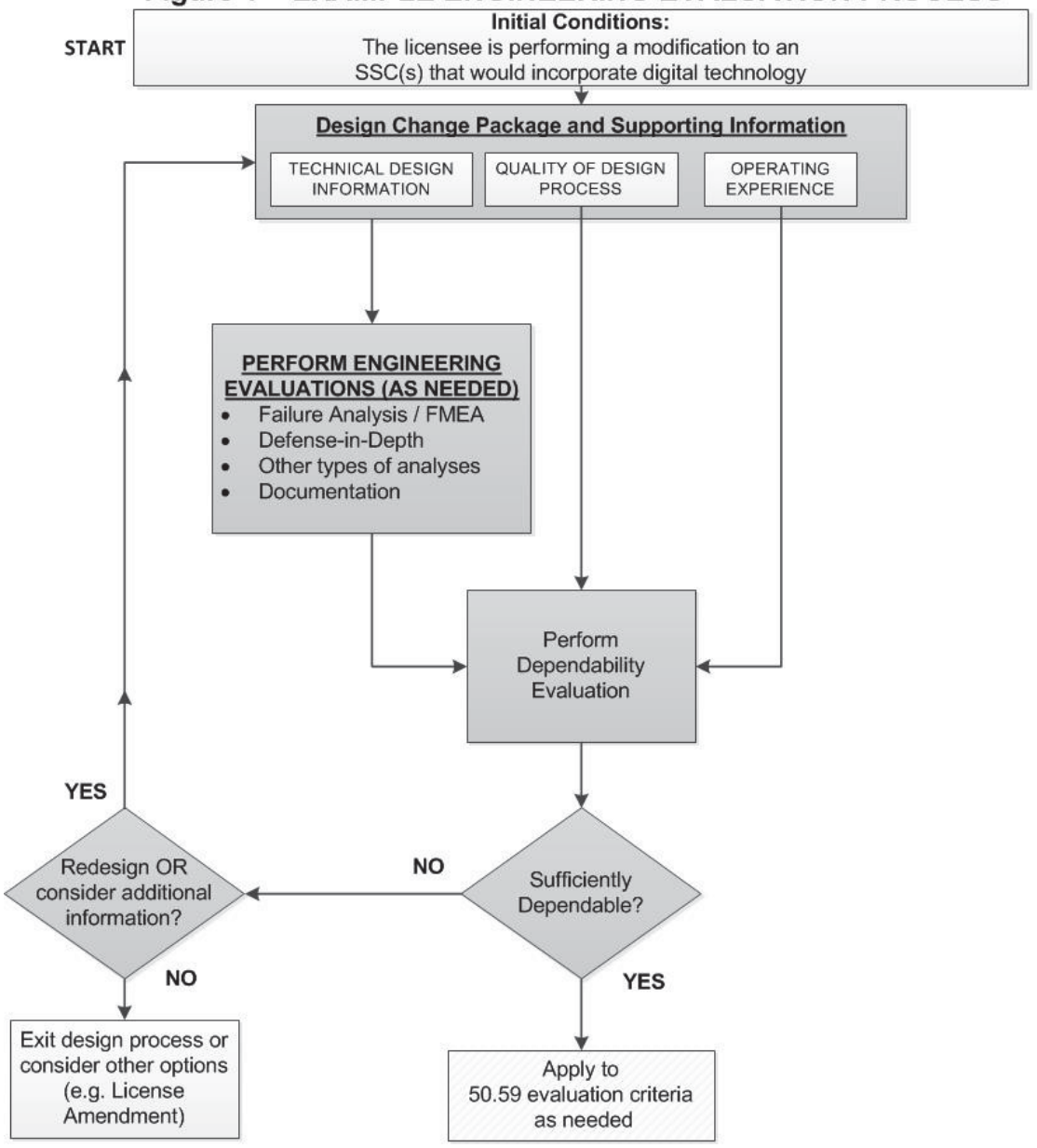
### 4.6 Engineering Documentation

Documentation for a proposed digital I&C modification is developed and retained in accordance with the licensee's design engineering procedures, and the NRC-approved QA program. The documentation of an engineering evaluation identifies the possible failures introduced in the design and the effects of these failures. It also identifies the design features and/or procedures that document resolutions to identified failures, as described in NEI 01-01, Section 5.1.4. The level of detail used may be commensurate with the safety significance and complexity of the modification in accordance with licensee's procedures.

Although not required, licensees may use Table 2 of this attachment to develop and document engineering evaluations. Documentation should include an explanation providing adequate bases for conclusions so that a knowledgeable reviewer could draw the same conclusion.

807

**Figure 1 – EXAMPLE ENGINEERING EVALUATION PROCESS**




Note: This example presumes the proposed modification has 'screened in' for an evaluation under 10 CFR 50.59

Completed as part of technical design process

Completed as part of the 50.59 evaluation

808

809
810

| Table 2 Example - Engineering Evaluation Documentation Outline to support a Qualitative Assessment | |
|---|---|
| Topical Area | Description |
| Step 1- Identification | Describe the full extent of the SSCs to be modified boundaries of the design change, interconnections with other SSCs, and potential commonality to vulnerabilities with existing equipment.<br>• What are all of the UFSAR-described design functions of the upgraded/modified components within the context of the plant system, subsystem, etc.?<br>• What design function(s) provided by the previously installed equipment are affected and how will those design functions be accomplished by the modified design? Also describe any new design functions that were not part of the original design.<br>• What assumptions and conditions are expected for each associated design function? For example, the evaluation should consider both active and inactive states, as well as transitions from one mode of operation to another. |
| Step 2 Identify potential failure modes and undesirable behavior | Consider the possibility that the proposed modification may have introduced potential failures.<br>• Are there potential failure modes or undesirable behaviors as a result of the modification? A key consideration is that undesirable behaviors may not necessarily constitute an SSC failure, but a misoperation. (e.g., spurious actuation)<br>• Are failures including, but not limited to, hardware, software, combining of functions, shared resources, or common hardware/software considered?<br>• Are there interconnections or interdependencies among the modified SSC and other SSCs?<br>• Are there sources of CCF being introduced that are also subject to common triggering mechanisms with those of other SSCs not being modified?<br>• Are potential failure modes introduced by software tools or programmable logic devices? |
| Step 3 Assess the effects of identified failures | • Could the possible failure mode or undesired behavior lead to a plant trip or transient?<br>• Can the possible failure mode or undesired behavior affect the ability of other SSCs to perform their design function?<br>• Could the possible failure mode of the SSC, concurrent with a similar failure of another SSC not being modified but sharing a common failure and triggering mechanism affect the ability of the SSC or other SSCs to perform their design functions?<br>• What are the results of the postulated new failure(s) of the modified SSC(s) compared to previous evaluation results described in the UFSAR? |
| Step 4 Identify appropriate | What actions are being taken (or were taken) to address significant identified failures?<br>• Are further actions warranted? |

811

| Table 2 Example - Engineering Evaluation Documentation Outline to support a Qualitative Assessment | |
|---|---|
| Topical Area | Description |
| resolutions for each identified failures | • Is re-design warranted to add additional design features or attributes?<br>• Is the occurrence of failure self-revealing or are there means to annunciate the failure or misbehavior to the operator? |
| Step 5 Documentation | • Describe the resolutions identified in Step 4 of this table that address the identified failures.<br>• Describe the conformance to regulatory requirements, plant's UFSAR, regulatory guidance, and industry consensus standards (e.g., seismic, EMI/RFI, ambient temperature, heat contribution).<br>• Describe the quality of the design processes used within the software life cycle development (e.g., verification and validation process, traceability matrix, quality assurance documentation, unit test and system test results).<br>• Describe relevant operating history (e.g., platform used in numerous applications worldwide with minimal failure history).<br>• Describe the design features/attributes that support the dependability conclusion (e.g., internal design features within the digital I&C architectures such as self-diagnostic and self-testing features or physical restrictions external to the digital I&C portions of the modified SSC), defense-in-depth (e.g., internal diversity, redundancy, segmentation of distributed networks, or alternate means to accomplish the design function).<br>• Summarize the results of the engineering evaluation including the dependability determination. |

**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 DATE: Month XX, 2018**

| | | | | |
|---|---|---|---|---|
| **OFFICE** | NRR/DIRS/IRGB/PM | NRR/PMDA | OE/EB | OCIO |
| **NAME** | TGovan | LHill | JPeralta | DCullison |
| **DATE** | 02/16/2018 | 01/18/2018 | 01/22/2018 | 01/17/2018 |
| **OFFICE** | NRR/DE/EICB/BC | NRR/DIRS/IRGB/LA | NRR/DIRS/IRGB/PM | NRR/DIRS/IRGB/BC |
| **NAME** | MWaters | ELee | TGovan | HChernoff |
| **DATE** | 03/01/2018 | 02/22/2018 | 03/01/2018 | 03/01/2018 |

**Industry Suggested Revision to RIS 2017-XX Section 3.1.3 - Operating Experience**

### 3.1.3 Operating Experience

Relevant operating experience can be used to help evaluate and demonstrate that software and hardware employed in a proposed modification have adequate dependability. The licensee may document information showing that the proposed system or component modification employs equipment with significant operating experience in nuclear power plant applications, or in non-nuclear applications with comparable performance standards and operating environment. With a large population of in-service components/systems, operating experience provides a large installed test bed with many different environments and applications.

Operating experience is normally used in two basic ways 1) calculation of an actual failure rate number, or 2) a qualitative method that mines the failure data for both positives and negatives. Failure rate numbers based upon real performance data is the best quality indicator and calculated failure rate numbers can provide a comparison to the plant's existing components/systems. Qualitative methods involve review of the actually reported failure descriptions. These reviews can provide supporting evidence and trends of strengths or weaknesses in the manufacture's quality processes, such as design control processes, product testing effectiveness, and hardware robustness. The licensee may also consider whether the manufacturer of such equipment incorporate quality processes such as continual process improvement, incorporation of lessons learned, etc., and document how that information demonstrates adequate equipment dependability.

Some key areas in evaluating operating experience are:

- Strength of the manufacture's problem reporting system
- Identification of the manufacture's threshold for problem reporting and how this information is utilized (i.e. how problems are tracked, are critical problems fixed in a timely manner, is data used for continuous improvement)
- Evaluating for repetitive failure trends which could be indicative of a process weakness that requires further evaluation.
- Evaluate different revisions and versions of hardware/software for issues that occur during design or manufacturing changes.
- How "no problem found" is addressed and how large is this population.

Operating experience relevant to a proposed digital I&C change may be credited as part of an adequate basis for a determination that the proposed change does not result in more than a minimal increase in the frequency of occurrence of initiating events that can lead to accidents or in more than a minimal increase in the likelihood of occurrence of a malfunction of an SSC important to safety previously evaluated in the UFSAR. Differences may exist in the specific digital I&C application between the proposed digital I&C modification and that of the equipment and software whose

**Deleted:** Section 5.3.1 of NEI 01-01 states, "Substantial applicable operating history reduces uncertainty in demonstrating adequate dependability."¶
¶
Consistent with the above-quoted text, r

**Deleted:** is

**Deleted:** s

**Deleted:** but

**Deleted:** As for the q

**Deleted:** , this

**Deleted:** s

**Deleted:** either good

**Deleted:** sometimes

**Deleted:** , etc

**Deleted:** suppliers

**Formatted:** Bulleted + Level: 1 + Aligned at: 0.63" + Indent at: 0.88"

**Deleted:** ;

**Formatted:** Indent: Left: 0.38"

**Deleted:** What is

**Formatted** ... [1]

**Deleted:** s

**Deleted:** what is done

**Deleted:** with this

**Deleted:** utlized

**Deleted:** e.g.,

**Deleted:** is

**Deleted:** are

**Deleted:** there

**Deleted:** ing

**Deleted:** , etc.

**Deleted:** ¶

**Formatted:** Indent: Left: 0.38"

**Formatted:** Font: 11 pt

**Formatted** ... [2]

**Deleted:** problem or

**Formatted:** Font: 11 pt

**Deleted:** be possible

**Deleted:** sign of

**Formatted:** Font: 11 pt

**Formatted:** Indent: Left: 0.38"

**Formatted** ... [3]

**Formatted:** Indent: Left: 0.38"

**Formatted** ... [4]

operating experience is being credited. The architecture of the referenced equipment and software should be similar to that of the system being proposed. Note that an evaluation of multiple versions can provide evidence of good and stable design and manufacturing processes.

Further, the design conditions and modes of operation of the equipment whose operating experience is being referenced also needs to be similar to that being proposed as a digital I&C modification. It is important to recognize that when crediting operating experience, one needs to understand what design features are being credited. Highly-configurable components/systems may require a larger population of in-service data to address the potential different applications. Customized or rarely used functions should be avoided in operating experience evaluations. Design features that serve to prevent or limit possible common cause failures as relevant operating experience should be noted and considered for inclusion in the proposed design. Doing so would provide additional support for a determination that the dependability of the proposed design will be similar to the referenced application.

**Deleted:** In all cases, however, t

**Deleted:** substantially

**Deleted:** substantially

**Deleted:** For example, one needs to understand what operating conditions (e.g., ambient environment, continuous duty, etc.) were experienced by the referenced design. In addition, i

**Deleted:** i

**Deleted:** from other facilities

**Deleted:** were present in the design whose operating experience is

**Deleted:** Note that the more user-h

**Deleted:** thea

**Deleted:** is meansindicates that

**Deleted:** ismay be needed

**Deleted:** cover

**Deleted:** onal

**Deleted:** in a design referenced

| Page 1: [1] Formatted | Author |
| --- | --- |

Bulleted + Level: 1 + Aligned at:  0.63" + Indent at:  0.88"

| Page 1: [2] Formatted | Author |
| --- | --- |

Bulleted + Level: 1 + Aligned at:  0.63" + Indent at:  0.88"

| Page 1: [3] Formatted | Author |
| --- | --- |

Bulleted + Level: 1 + Aligned at:  0.63" + Indent at:  0.88"

| Page 1: [4] Formatted | Author |
| --- | --- |

Bulleted + Level: 1 + Aligned at:  0.63" + Indent at:  0.88"

**Industry Suggested Revision to Table 2 of RIS 2017-XX**

| **Table 2—Example Engineering Evaluation Documentation Outline to Support a Qualitative Assessment** | |
|---|---|
| Topical Area | Description |
| Step 1— Activity Identification | • Describe the scope and boundaries of the proposed activity including interconnections with other SSCs.<br>• List the UFSAR-described design function(s) affected by the proposed change.<br>• Describe any new design functions performed by the modified design that were not part of the original design.<br>• Describe any design functions eliminated from the modified design that were part of the original design.<br>• Describe any previously separate design functions that were combined as part of the activity.<br>• Describe any automatic actions to be transferred to manual control.<br>• Describe any manual actions that are to be transferred to automatic control. |
| Step 2—Failure Mode Comparison | • Provide a comparison between the failure modes of the new digital equipment and the failure modes of the equipment being replaced.<br>• If the failure modes are different, describe the resulting effect of equipment failure on the affected UFSAR-described design function(s). |
| Step 3—Determination of Equipment Reliability and CCF Likelihood | Using the qualitative assessment categories provided in Table 1, address the following questions:<br>• Is the new digital equipment as reliable as the equipment being replaced?<br>• Is the new digital equipment CCF susceptibility much lower than the likelihood of failures considered in the UFSAR (e.g., single failures) and comparable to CCFs that are not considered in the UFSAR (e.g., design flaws, maintenance errors, calibration errors)? |
| Step 4—Assessment of Equipment Reliability and CCF Likelihood Results | **IF** the results of Step 3 indicate the new digital equipment is as reliable as the equipment being replaced **AND** CCF likelihood is determined to be sufficiently low, perform the following:<br>• Document that no new plant-level vulnerabilities were identified (i.e., the proposed activity will not increase accident frequency/malfunction likelihood or create an accident of a different type/malfunction with a different result)<br>• Continue to Step 5<br>**IF** the results of Step 3 indicate the new digital equipment is not as reliable as the equipment being replaced, perform the following:<br>• Using the guidance provided in NEI 96-07, Rev. 1, Section 4.3.1 and Section 4.3.2, determine if the decrease in reliability will result in more than a minimal increase in accident frequency or malfunction likelihood and document the justification.<br>**IF** the results of Step 3 indicate the CCF likelihood is not sufficiently low, perform the following:<br>• Using the guidance provided in NEI 96-07, Rev. 1, Section 4.3.5 and Section 4.3.6, determine if a postulated CCF will result in a different type of accident or a malfunction with a different result and document the justification. |

| Table 2—Example Engineering Evaluation Documentation Outline to Support a Qualitative Assessment | |
|---|---|
| Topical Area | Description |
| Step 5—Conclusion | Provide a summarization of the qualitative assessment results and overall conclusions reached. Include a discussion of the pros and cons associated with implementation of the proposed activity (e.g., elimination of single points of vulnerability, self-diagnostics and testing). Discuss the effect of the proposed activity, if any, on applicable UFSAR-described design functions. Provide discussion on any differences in equipment failure modes and the associated impact of different failure modes on applicable UFSAR-described design functions. |
| Step 6—Supporting Documentation | Provide a list of references used to support arguments made and conclusions reached in the qualitative assessment. References should be retrievable for future review and inspection activities. If not retrievable, consider attaching references to the qualitative assessment. The level of supporting documentation should be commensurate to the safety significance of the SSCs being modified.<br>Examples of references include:<br>• Applicable codes and standards applied in the design<br>• Equipment environmental qualifications (e.g., ambient temperature, EMI/RFI, seismic)<br>• Quality design processes employed (e.g., NQA-1, Part II, Subpart 2.7; Commercial Grade Dedication documentation per EPRI TR-106439)<br>• Failure Modes and Effects Analysis (if applicable)<br>• Software Hazard Analysis (if applicable)<br>• Critical Digital Reviews (if applicable)<br>• Documentation of equipment operating experience |
| Step 7—Application of Qualitative Assessment Results | • Apply the qualitative assessment results when responding to the 10 CFR 50.59 Evaluation questions.<br>• List the qualitative assessment as a reference (or include as an attachment) to the 10 CFR 50.59 Evaluation. |