NRR-DMPSPEm Resource

From: Ken Scarola <KenScarola@NuclearAutomation.com>
Sent: Monday, May 22, 2017 11:00 PM
To: Drake, Jason
Cc: Rahn, David; Morton, Wendell; Waters, Michael
Subject: [External_Sender] Comments on Draft RIS
Attachments: NRC-RIS17xx-Draft-05-19-17-ML17139C181_KS R1.pdf

Jason,
Attached are my comments on the "advance version" of the RIS that was transmitted by Mike Waters on Friday May 19th to support the publice meeting (workshop) on May 25th. I am sending these comments, because I had previous plans to be on vacation during the time the official version is being distributed publically via the FRN for public comments. Thank you for considering my comments.

Ken

_____

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

Hearing Identifier: NRR_DMPS
Email Number: 190

Mail Envelope Properties (006101d2d370$abbd1820$03374860$)

Subject: [External_Sender] Comments on Draft RIS
Sent Date: 5/22/2017 10:59:57 PM
Received Date: 5/22/2017 11:00:14 PM
From: Ken Scarola

Created By: KenScarola@NuclearAutomation.com

Recipients:
"Rahn, David" <David.Rahn@nrc.gov>
Tracking Status: None
"Morton, Wendell" <Wendell.Morton@nrc.gov>
Tracking Status: None
"Waters, Michael" <Michael.Waters@nrc.gov>
Tracking Status: None
"Drake, Jason" <Jason.Drake@nrc.gov>
Tracking Status: None

Post Office: NuclearAutomation.com

Files	**Size**	**Date & Time**
MESSAGE	559	5/22/2017 11:00:14 PM
NRC-RIS17xx-Draft-05-19-17-ML17139C181_KS R1.pdf	479255	

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

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

May XX, 2017

NRC DRAFT REGULATORY ISSUE SUMMARY 2017-XX
CLARIFICATION OF THE NRC STAFF ENDORSEMENT ON THE USE OF EPRI/NEI JOINT TASK FORCE REPORT, "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"
(REPORT PREVIOUSLY ENDORSED IN RIS 2002-22)

ADDRESSEES

All holders and applicants for power reactor operating licenses or construction permits under 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities," except those who have permanently ceased operations and have certified that fuel has been permanently removed from the reactor vessel.

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

INTENT

The U.S. Nuclear Regulatory Commission (NRC) is issuing a supplement to the NRC staff's endorsement of the Electric Power Research Institute (EPRI)/Nuclear Energy Institute (NEI) Joint Task Force report entitled, "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," (hereinafter referred to as "NEI 01-01") (Agencywide Documents Access and Management System (ADAMS) Accession No. ML020860169.) In addition, the staff is providing guidance in documenting the basis for the determination that the proposed change under 10 CFR 50.59 does not require a license amendment. In Regulatory Issue Summary (RIS) 2002-22, dated November 25, 2002 (ADAMS) Accession No. ML023160044), the NRC staff endorsed the use of NEI 01-01 for designing, licensing, and implementing digital upgrades and replacements to instrumentation and control (I&C) systems in a consistent and comprehensive manner.

This RIS is not intended to supersede or replace RIS 2002-22. Rather, this RIS clarifies the NRC staff's endorsement of the guidance in NEI 01-01 for preparing and documenting qualitative assessments that provide the basis for the 10 CFR 50.59 evaluation of whether the change requires a license amendment pursuant to 10 CFR 50.90.

The attachment to this RIS clarifies the guidance in NEI 01-01 in Section's 4, 5, and Appendix A for documenting the bases for the determination that a modification does not require a license amendment. The attachment also clarifies NRC's endorsement of NEI 01-01 with respect to the

performance and documentation of the qualitative assessments necessary to support a 10 CFR 50.59 determination. Licensees should apply the qualitative assessment methodology described in the attachment when preparing the written evaluation of 10 CFR 50.59(c)(2) criteria.

The guidance in this RIS applies only to a limited subset of digital I&C technology upgrades, as described below in the "Scope of Applicability of Qualitative Assessment Guidance Clarifications" section.

Because this RIS may overlap with the guidance in RIS 2002-22, it is possible that licensees may encounter apparent conflicts between the two documents. In such cases, licensees should follow this RIS, as the most recent source of guidance.

This RIS provides clarity regarding the NRC staff's endorsement of NEI 01-01 for use in implementing digital I&C changes to licensed nuclear power plants that are initiated after issuance of this RIS.

This RIS 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 (GL) 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 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, standard design certifications, and operating licenses have used this guidance, in support of the digital design modifications, in conjunction with Regulatory Guide (RG) 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 Evaluations," Revision 1, dated November 2000 (ADAMS Accession No. ML003771157).

Clause (d)(1) of 10 CFR 50.59 states: "The licensee shall maintain records of changes in the facility, of changes in procedures, and of tests and experiments made pursuant to paragraph (c) of this section. These records must include a written evaluation which provides the bases for the determination that the change, test, or experiment does not require a license amendment pursuant to paragraph (c)(2) of this section."

Since the issuance of RIS 2002-22, NRC inspections of plant digital modifications performed under 10 CFR 50.59 revealed that some licensees have encountered difficulties in applying the guidance and acceptance criteria within other applicable technical guidance documents while conforming to the guidance of NEI 01-01 and subsequently performing effective evaluations as required by 10 CFR 50.59. NRC staff inspections of design modifications performed by some

licensees have also identified concerns with the analyses developed by the licensees to support their determinations under 10 CFR 50.59 that a license amendment is not required for these modifications. For example, NRC inspectors identified cases where licensees did not adequately document how the application of codes and standards was considered appropriate to support the determination that a license amendment was not required.

In response to Staff Requirements Memorandum (SRM)-SECY-16-0070 "Integrated Strategy to Modernize the Nuclear Regulatory Commission's Digital Instrumentation and Control Regulatory Infrastructure" ADAMS Accession No. ML16299A157), NRC staff has undertaken continued engagement with NEI and industry representatives to improve the guidance for justifying digital I&C-related design modifications under the 10 CFR 50.59 process as part of a broader effort to modernize the I&C regulatory infrastructure. This modernization plan also includes evaluating the effects of potential digital-technology-induced common cause failures (CCF) on nuclear power plant safety. The NRC staff's plan for accomplishing this update is outlined in the NRC's "Integrated Action Plan to Modernize Digital Instrumentation and Controls Regulatory Infrastructure" (ADAMS Accession No. ML17102B307), including the planned schedule for completion of key infrastructure improvements. As part of this plan, the NRC staff and stakeholders have identified an immediate need for clarification of the NRC staff's guidance for performing adequate 10 CFR 50.59 evaluations associated with planned digital I&C modernization projects. This RIS is intended to fulfill that need.

SUMMARY OF ISSUE

In addition to providing technical criteria for appropriately implementing digital I&C technology, NEI 01-01 provides criteria for addressing the 10 CFR 50.59 evaluation. The guidance in NEI 01-01 provides for a technical (deterministic) assessment of the capabilities of a proposed design change, as well as the performance and documentation of appropriately prepared qualitative assessments for supporting determinations as to the likelihood of new digital I&C malfunctions. Adequate performance and documentation of such assessments is important for supporting the development of responses to the eight criteria required to be addressed under 10 CFR 50.59(c)(2)(i) through (viii).

This RIS clarifies NRC's endorsement of the guidance within NEI 01-01 pertaining to the development of adequate technical evaluations and adequately documented qualitative assessments for use in conjunction with proposed system and component upgrades using digital I&C technology to address the requirements of 10 CFR 50.59. The attachment to this RIS provides clarification of the NRC staff's endorsement of NEI 01-01 as it relates to the performance and documentation of the qualitative assessment aspects of 10 CFR 50.59 evaluations.

Scope of Clarifications

This RIS is limited to the types of digital I&C modifications with characteristics indicating they are less safety significant and easier to analyze. In specifying the characteristics described below, this RIS limits the scope of proposed digital I&C modifications to those which: a) would not compromise independence or diversity; b) would not introduce a potential for a new failure that would be required to be considered within the design basis (i.e., no shared resources); and c) can be shown to have such a likelihood of a design defect that would be considered to be much lower than that of single failures already considered in the design basis, or treated as

"beyond design basis," or capable of demonstration that the resulting replacement or upgrade design can tolerate the postulated triggering of that defect.

In the list of characteristics below, "design functions" are the functions within the same system as described in the licensing basis, including components and systems not explicitly described in the final safety analysis report (FSAR), but which specifically support the functions of the described system. Proposed digital I&C technology changes to other plant systems or components that do not meet the criteria listed above can still be pursued under the guidance of RIS 2002-22 for proposed changes under the 10 CFR 50.59 process or be submitted to the NRC staff for evaluation under the 10 CFR 50.90 process.

Provided licensees prepare and document written evaluations of the criteria in 10 CFR 50.59 by using the attachment to this RIS, licensees should be able to implement digital modifications with the characteristics listed below:

1. Digital I&C technology function-for-function replacements and upgrades to systems and components that:

    - Do not result in the integration of systems, subsystems, or components that combine design functions not previously combined within the same system, subsystem, or component being replaced, and
    - Do not have shared resources (such as power supplies, controllers, and human-machine interfaces) with other system functions credited in the FSAR as functioning independently from other plant system functions.

    "Integration" refers to the process of combining software components, hardware components, or both into an overall system, or the merger of the design bases of two or more systems or components into a functioning and unified higher-level system or component. Specifically, the scope of this RIS includes potential upgrades to portions of safety and non-safety systems (other than RPS and ESF actuation systems) that do not result in the design functions from different systems (as described in the licensing basis) being integrated or combined (either directly in the same digital device or indirectly via shared resources, such as direct digital communications or networks, or visual display units) into the integrated functions of a proposed new control system, safety-related distributed monitoring system, or component.

2. Digital I&C technology replacements and upgrades to systems and components that do not alter any aspects of functional diversity credited in the FSAR for systems that have specific diversity requirements as described in the licensing basis.

3. Digital I&C technology upgrades to facility components and systems associated with RPS and ESF actuation systems that are not a part of the actuation logic portion of RPS and ESF actuation systems, provided the proposed change does not reduce channel, division, or train independence, as described in the licensing basis. For example, changes to individual, non-shared channel inputs to RPS logic, RPS power supplies, or output actuators (relays/breakers) are within scope, provided the licensing basis independence and single failure criteria are maintained, and any new input or output devices do not communicate with the actuation logic portion of RPS or ESF actuation systems using digital data communications.

4. Other plant system or component level equipment replacements that maintain the licensing basis independence (or separation) and single failure criteria.

Clarification of Guidance for Addressing Digital I&C Changes under 10 CFR 50.59

NEI 01-01 contains several references to key sections within NEI 96-07, Revision 1. NEI 96-07 supports the use of qualitative assessments, qualitative engineering judgment, and/or industry precedent when addressing whether the frequency of malfunctions occurring would be more than minimally increased, or whether a possibility for a malfunction of a system or component important to safety has been introduced that could alter the conclusions of the safety analysis.

The clarified endorsement in this RIS identifies the need to document how the implementation of key design attributes and quality management measures is being credited in demonstrating a sufficient reduction in uncertainty when performing qualitative assessments of the likelihood of occurrence of potential malfunctions for proposed modifications having the key design characteristics listed in the "Scope of Clarifications" section above. While the guidance in NEI 01-01 provides a "road map" to relevant standards and other sources of detailed guidance, this RIS identifies how the potential effectiveness of the design features and quality management measures that are applied to the proposed design using such standards and guidance should be described and evaluated within licensee documentation, including the reasoning needed to support a licensee's conclusion that the residual uncertainty does not affect the determination that a license amendment is not needed.

To assist licensees in preparing acceptable qualitative assessments supporting the rationale for responding to the 10 CFR 50.59(c)(2) criteria, the NRC staff has clarified within the attachment to this RIS its position on the minimum content, rationale, and evaluation factors that should be addressed and evaluated within licensee-developed qualitative assessments that contribute to the justification for the determination that the change does not require a license amendment. Specifically, the clarification within the attachment describes the NRC staff expectations for such qualitative assessments to clearly demonstrate an adequate technical basis for the determination that the change does not require prior NRC staff approval. Such conclusions should be based on evidence (i.e., adequate design measures, quality processes, and an evaluation of relevant operating experience) through reasoning demonstrating how the evidence contributed to the conclusions, commensurate with the level of safety significance of the proposed modification or potential severity of the consequences of potential malfunctions.

Section 3.2.3 of the NRC staff's evaluation of NEI 01-01 (Attachment 1 of RIS 2002-22) states:

> The staff's position regarding documentation of 10 CFR 50.59 evaluations is accurately reflected in the second paragraph in Appendix A to the submittal, which states: "The 10 CFR 50.59 questions should be answered in sufficient detail, either by reference to a source document or by direct statements, that an independent third party can verify the judgements." The staff has reviewed Appendix A, "Supplemental Questions for Addressing 10 CFR 50.59 Evaluation Criteria," and Appendix B, "Outline for Documenting 10 CFR 50.59 Screens and Evaluations," and, based on the foregoing, concludes that the guidance therein is acceptable for licensees to use in performing and documenting their 10 CFR 50.59 evaluations.

This RIS clarifies the above statement regarding the acceptability of the guidance within Appendices A and B of NEI 01-01. Specifically, the clarifications within this RIS are intended to apply to the documentation aspects of the condition in the above statement that "the 10 CFR 50.59 questions should be answered in sufficient detail, either by reference to a source document or by direct statements, that an independent third party can verify the judgements." (Reference 10 CFR 50.59(d)(1))

BACKFITTING AND ISSUE FINALITY DISCUSSION

[PER GEARY MIZUNO, OGC WILL PROVIDE THIS DISCUSSION]

***FEDERAL REGISTER* NOTIFICATION**

[Discussion to be provided in final RIS.]

CONGRESSIONAL REVIEW ACT

[Discussion to be provided in final RIS.]

PAPERWORK REDUCTION ACT STATEMENT

This Regulatory Issue Summary contains information collection requirements that are subject to the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et seq.). These information collections were approved by the Office of Management and Budget, approval number 3150-0011.

The burden to the public for these mandatory information collections is estimated to average 16 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the information collection. 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.

Tim McGinty, Director
Division of Construction Inspection
and Operation Programs
Office of New Reactors

Louise Lund, Director
Division of Policy and Rulemaking
Office of Nuclear Reactor Regulation

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

Wendell Morton, NRO
301-415-1315
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: Davie.Beaulieu@nrc.gov

Lead Project Manager Contact: Brian Harris, NRR
301-415-2277
e-mail: Brian.Harris2@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: Draft Qualitative Assessment Framework

Draft Qualitative Assessment Framework

1. Introduction

2. Purpose

This attachment clarifies the NRC staff's endorsement of NEI 01-01 guidance for performing and documenting qualitative assessments to support Title 10 of the *Code of Federal* Regulations (10 CFR) Section 50.59 evaluations for proposed digital I&C systems modifications. These qualitative assessments are needed to document the technical bases to support a conclusion that there is reasonable assurance that a proposed digital I&C modification has a sufficiently low likelihood of failure, consistent with Final Safety Analysis Report (as updated) (UFSAR) analysis assumptions. This conclusion is used in the 10 CFR 50.59 written evaluation to determine whether prior NRC approval is required prior to a digital I&C system modification.

A qualitative assessment can support the following conclusions:

- The activity does not result in more than a minimal increase in the frequency of occurrence of an accident previously evaluated in the UFSAR (10 CFR 50.59(c)(2)(i)).
- The activity does not result in more than a minimal increase in the likelihood of occurrence of a malfunction of a structure, system, or component (SSC) important to safety previously evaluated in the UFSAR (10 CFR 50.59(c)(2)(ii)).
- The activity does not result in more than a minimal increase in the consequences of an accident previously evaluated in the UFSAR (10 CFR 50.59(c)(2)(iii)).
- The activity does not result in more than a minimal increase in the consequences of a malfunction of an SSC important to safety previously evaluated in the UFSAR (10 CFR 50.59(c)(2)(iv)).
- The activity does not create a possibility for an accident of a different type than any previously evaluated in the UFSAR (10 CFR 50.59(c)(2)(v)).
- 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 (10 CFR 50.59(c)(2)(vi)).

For digital modifications under 10 CFR 50.59, licensees have experienced challenges in responding to criterion 10 CFR 50.59(c)(2)(i), (ii), (v), and (vi).

The ability to provide reasonable assurance that the digital modification will exhibit a low likelihood of failure is a key element of 10 CFR 50.59 evaluations of whether the change requires prior NRC approval. To support the 10 CFR 50.59 process, methods are needed to evaluate digital system likelihood of failure (e.g., based on reliability, dependability of the modified digital components). For digital systems, there may be no well-established, accepted quantitative methods that can be used to estimate reliability or likelihood of failure. Therefore, for digital systems, reasonable assurance of low likelihood of failure is derived from a qualitative assessment of factors involving system design features, the design process, and the operating history (i.e., product maturity and in-service experience). The qualitative assessment reaches a final determination there is reasonable assurance that the digital modification will exhibit a low likelihood of failure by considering the aggregate of these factors. This final determination of the

likelihood of failure is key element of the evaluation of criteria 10 CFR 50.59(c)(2)(i), (ii), (v) and (vi).[1]

The description of low likelihood of failure (i.e., the "likelihood threshold") is tailored to criteria 10 CFR 50.59(c)(2)(i), (ii), (v) and (vi). The qualitative assessment should reach a final determination that the proposed digital modification satisfies the each of these likelihood thresholds.

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

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?

> Likelihood threshold – The activity does not increase the likelihood of failure of equipment that causes a more than minimal increase the frequency of initiating events that lead to accidents 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 previously evaluated in the UFSAR?

> Likelihood threshold – The activity does not result in more than a minimal increase in the likelihood of 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 50, Appendix B).

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

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?

> Likelihood threshold – The activity does not create a possibility for an accident of a different type than any previously evaluated in the UFSAR because: possible accidents of a different type are limited to those that are as likely to happen as those previously evaluated in the UFSAR; and, based on the likelihood of failure of equipment that can initiate events that lead to accidents that are of different type, the activity does not create an accident of a different type that is as likely to happen as those previously evaluated in the UFSAR.

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?

[1] Paragraph derived from NEI 01-01, Section 5.3.1, "Factors that Affect Dependability."

Likelihood threshold – The activity does not create a possibility for a malfunction of an SSC important to safety with a different result based on: possible malfunctions with a different result are limited to those that are as likely to happen as those described in the UFSAR; and, there is reasonable assurance the likelihood of CCF is much lower than the likelihood of failures that are considered in the UFSAR (e.g., single failures) and comparable to other CCF that are not considered in the UFSAR (e.g., design flaws, maintenance errors, calibration errors). [Note: This likelihood threshold is not interchangeable with that for "credible"/"not credible" which has a threshold of "as likely as" (i.e., not "*much lower" than*) malfunctions already assumed in the UFSAR.]

The above likelihood thresholds were 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.

For activities that introduce a potential failure mode (e.g., CCF) that meets the above conditions, the CCF alone would not require the change to be approved under 10 CFR 50.90 through a license amendment request.

For activities that introduce a potential failure mode (e.g., CCF) that does not meet the above conditions, the CCF would need to become part of the licensing basis; a license amendment or other approved process would be required.

This qualitative assessment framework is intended to clarify, rather than replace the guidance provided for qualitative assessments that are described in NEI 01-01.

3. Qualitative Assessment

3.1. Quantitative vs. Qualitative

A quantitative assessment is one capable of representing the SSC by a mathematical model, such as apportioning the reliability and availability goals among parts of the system, assigning probabilities to each failure mode of concern, and reconciling the calculated estimates of reliability and availability with the over-all SSC goals. A qualitative assessment identifies possible ways in which a SSC can fail, and identifies appropriate precautions (design changes, administrative procedures, etc.) that will reduce the frequency or consequences of such failures. For example, electrical independence can be demonstrated quantitatively, by showing that where electrical connections are necessary, the probability of a fault occurring or that the fault propagating between SSCs is either not credible, or has extremely low likelihood of occurrence, or for which the likelihood of credible damage resulting is extremely low, and therefore additional precautions may not be necessary. Alternatively, electrical independence can be demonstrated qualitatively by showing that where electrical connections are necessary, an isolation device can be used as a precaution to reduce the frequency or consequences of such failures.

3.2. Qualitative Assessment Categories

In addition to qualitative assessment preparation methods for evaluating dependability/reliability and performing failure analyses specified in appropriate quality standards, the qualitative

assessment framework specifies three general categories of proposed design-related characteristics (described in Table 1 of this qualitative assessment framework). Each category needs to be evaluated to formulate adequate qualitative justifications deemed sufficient to address the criteria described in Section 2 above. The aggregate of the three qualitative assessment categories form the technical basis for developing justifications based upon the likelihood of failure (i.e., single failures and CCF) of a digital I&C modification to a system or components. The following categories should be evaluated in conjunction with the questions provided in NEI 01-01, Appendix A:

- Design attributes: 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.
    - Hardware and software design features that contribute to high dependability (See Section 5.3.4). Such 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."

Design attributes of the proposed modification should prevent or limit failures from occurring or mitigate the consequences of such possible failures. The assessment should document and describe 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 designed to minimize failure consequences and facilitate problem diagnosis. However, external design attributes, such as those resulting from incorporation of the proposed modification among the systems with which they act, should also be considered. Attributes of the proposed modification performing within the overall channel, train, system, or plant that serve to incorporates internal and external layers of defense against potential failures of the modified I&C system or component should be documented.

Documentation is needed to identify how the proposed design will respond appropriately to avoid creating modes of failure not already analyzed in the UFSAR or result in the initiation of a design basis Anticipated Operational Occurrence (AOO) or Postulated Accident (PA), or the initiation of new AOOs or PAs that have not been previously analyzed. Within the concept of layers of defense, acceptable justifications can be documented that the occurrence of a postulated failure is only possible after a sequence of multiple unlikely independent failures were to occur first. This type of justification should also be documented as part of the qualitative assessment.

- Quality processes: 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." Quality processes employed in the development of the proposed modification, should include software development, hardware and software integration processes, hardware design, and validation and testing processes that have been incorporated into the development process. "Quality Processes" does not imply 10 CFR

50 Appendix B requirements because Appendix B requirements apply only to those SSCs under the scope of that rule.

- Operating Experience: Section 5.3.1 of NEI 01-01 states, "Substantial applicable operating history reduces uncertainty in demonstrating adequate dependability." Evidence that the proposed system or component modification employs equipment with significant operating history in nuclear power plant applications or non-nuclear applications with comparable performance requirements, and the suppliers of such equipment incorporate quality processes such as continual process improvement, incorporation of lessons learned, etc.

These categories are not mutually exclusive and may overlap in certain areas. Adequate qualitative justifications for systems of varying safety significance should address the degree to which the proposed modification has addressed each of the above categories. All of these categories should be addressed and thoroughly documented within the licensee's QA program, in consideration of the safety significance of SSCs described below in Section 4.2. **(See Table 1.)**

Table 1 - Qualitative Assessment Categories	
Categories	Description
Design Attributes	• Design criteria—For example: Diversity (if applicable), Independence, and Redundancy. • Inherent design features for software, hardware or architectural/network—For example: external watchdog timers, isolation devices, segmentation, self-testing and self-diagnostic features. • Basis for identifying that possible triggers are non-concurrent. • Sufficiently Simple (i.e. enabling 100% testing). • Unlikely series of events—For example: evaluation of a given digital I&C modification would necessarily have to postulate multiple independent random failures in order to arrive at a state in which a CCF is possible. • Failure state always known to be safe.
Quality Processes	• Compliance with industry codes and standards - It is the expectation that for non-NRC endorsed codes and standards, the licensee must provide an explanation for why use of the particular non-endorsed standard(s) is acceptable. • Use of Appendix B vendors, or if not Appendix B, which generally accepted industrial quality program applies. • Environmental qualification (e.g., EMI/RFI, Seismic). • Development process rigor.
Operating Experience	• Wide range of operating history in similar applications, operating environments, duty cycles, loading, comparable configurations, etc., to that of the proposed modification). • History of lessons learned from field experience addressed in the design. • 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 commercial products used in different applications provides a higher likelihood of resolution of potential deficiencies.

3.2.1 Design Attributes to Reduce the Likelihood of Failure

Many system design and testing attributes, procedures, and practices can contribute to significantly reducing the likelihood of failure (e.g., CCF) by deterministically assessing the specific vulnerabilities through the introduction of failure modes (e.g., CCF) within a proposed modification and applying specific design attributes to address those vulnerabilities (see Table 1 above). An adequate qualitative justification regarding the likelihood of failure of a proposed modification would consist of a thorough description of the identified vulnerabilities of the proposed modification, the design attributes utilized to address the identified vulnerabilities, and a clear description explaining why the chosen design attributes are sufficient.

Changes in how requirements are met need to be evaluated to ensure that they do not result in a potential increase in likelihood of failure. In addition, there are some SSCs that have only minimal applicable criteria. These SSCs may have been implemented in a manner (i.e., relatively independently) such that only individual SSC malfunction or failure was considered in

the FSAR (as updated). If these individual SSCs are combined with (e.g., controlled by a common digital component) or coupled to (e.g., by digital communication) each other, then the potential new malfunction(s) and/or accident(s) must be evaluated under 10 CFR 50.59.

3.2.1.1 Digital Communications

The introduction of digital communication (between redundancies, echelons of defense-in-depth, or different safety classifications) that does not meet NRC endorsed guidance for communications independence (e.g., DI&C-ISG-04) would not be within scope of this RIS and the proposed modification should be pursued under other NRC-approved processes.

3.2.1.2 Combination of Functions

The combination of functions in a manner not previously evaluated or described in the FSAR (as updated) (that (i) can cause a plant transient, (ii) are credited for mitigating plant transients either directly or as an auxiliary support function, or (iii) are of different echelons of defense-in-depth) should be evaluated under 50.59. If the 50.59 evaluation determines that: (A) a new type of accident, (B) a malfunction with a new result, or (C) an unbounded malfunction or accident now exists due to the combining of functions creating new malfunctions, new inter-system interactions, etc., then the licensee has the option to re-design the proposed modification to meet the scope of this RIS or pursue other NRC-approved processes.

3.2.1.3 Design Specifics

It is not possible for generic guidance to anticipate all of the ways that a design can introduce failure and malfunction modes; therefore, the design attributes of each proposed modification must be reviewed against the applicable 10 CFR 50.59(c)(2) criteria. This is in addition to the other categories listed in Table 1.

3.2.2 Quality Design Processes – Use of Codes and Standards

Design attributes credited for meeting any criteria must be stipulated and documented as being achieved (e.g., GDC 1 - Quality Standards and Records, and 10 CFR 50.55(jj) – Conditions of Licenses):

GDC 1 -

(1) “Structures, systems, and components important to safety shall be designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions to be performed.”

(2) “Where generally recognized codes and standards are used, they shall be identified and assessed to determine their applicability, adequacy, and sufficiency and shall be supplemented or modified as necessary to assure a quality product in keeping with the required safety function.”

This sentence allows the use of “generally recognized codes and standards,” when appropriate, instead of requiring quality standards for all important to safety aspects. That is, codes and standards can be incorporated by reference in plant specific specifications of important to safety equipment. These standards could be a set of detailed technical guidelines, used as a means of establishing uniformity.

(3) "A quality assurance program shall be established and implemented in order to provide adequate assurance that these structures, systems, and components will satisfactorily perform their safety functions."

This sentence requires process controls for important to safety equipment that is not subject to an Appendix B QA program.

(4) "Appropriate records of the design, fabrication, erection, and testing of structures, systems, and components important to safety shall be maintained by or under the control of the nuclear power unit licensee throughout the life of the unit."

The sentence requires documentation for important to safety equipment that is not part of an Appendix B QA program.

10 CFR 50.54(jj) -

"Structures, systems, and components subject to the codes and standards in 10 CFR 50.55a must be designed, fabricated, erected, constructed, tested, and inspected to quality standards commensurate with the importance of the safety function to be performed."

This sentence references the requirement that SSCs be designed, tested, and installed to standards commensurate to importance of the safety function being performed, subject to 10 CFR 50.55a. Per 36 FR 11423-11428 – (Rulemaking for 10 CFR 50.55a, "Codes and Standards,") which is applicable to 10 CFR 50.54(jj), "Conditions of Licenses," it is stated, in part:

> "Regulations in 10 CFR Part 50, 'Licensing of Production and Utilization Facilities,' establish minimum quality standards for the design, fabrication, erection, construction, testing, and inspection of certain systems and components of boiling and pressurized water-cooled nuclear power reactor plants by requiring conformance with appropriate editions of published industry codes and standards…"
>
> "Criterion 1 of the 'General Design Criteria for Nuclear Power Plants' (Appendix A of Part 50) requires that structures, systems, and components of nuclear power plants which are important to safety be designed, fabricated, erected, and tested to quality standards that reflect the importance of the safety functions to be performed. It has been generally recognized that, for boiling and pressurized water-cooled reactors …that protection systems (electrical and mechanical sensors and associated circuitry) should, as a minimum, be designed to meet the criteria developed by the Institute of Electrical and Electronics Engineers (IEEE)."

The term "quality standards" is sometimes a source of confusion. The *Federal Register* notice above clarifies that for protection systems, otherwise known as safety-related electrical SSCs or Class 1E SSCs, quality standards means "codes and standards." At a minimum, these standards are documents established by consensus and approved by an accredited standards development organization that provides, for common and repeated use, rules, guidelines, or characteristics for

activities or their results, aimed at the achievement of the optimum degree of order and consistency in a given context, such as IEEE standards.

For SSCs that may be considered important to safety, but not considered Class 1E, GDC 1 Clause (2) above would be applicable.

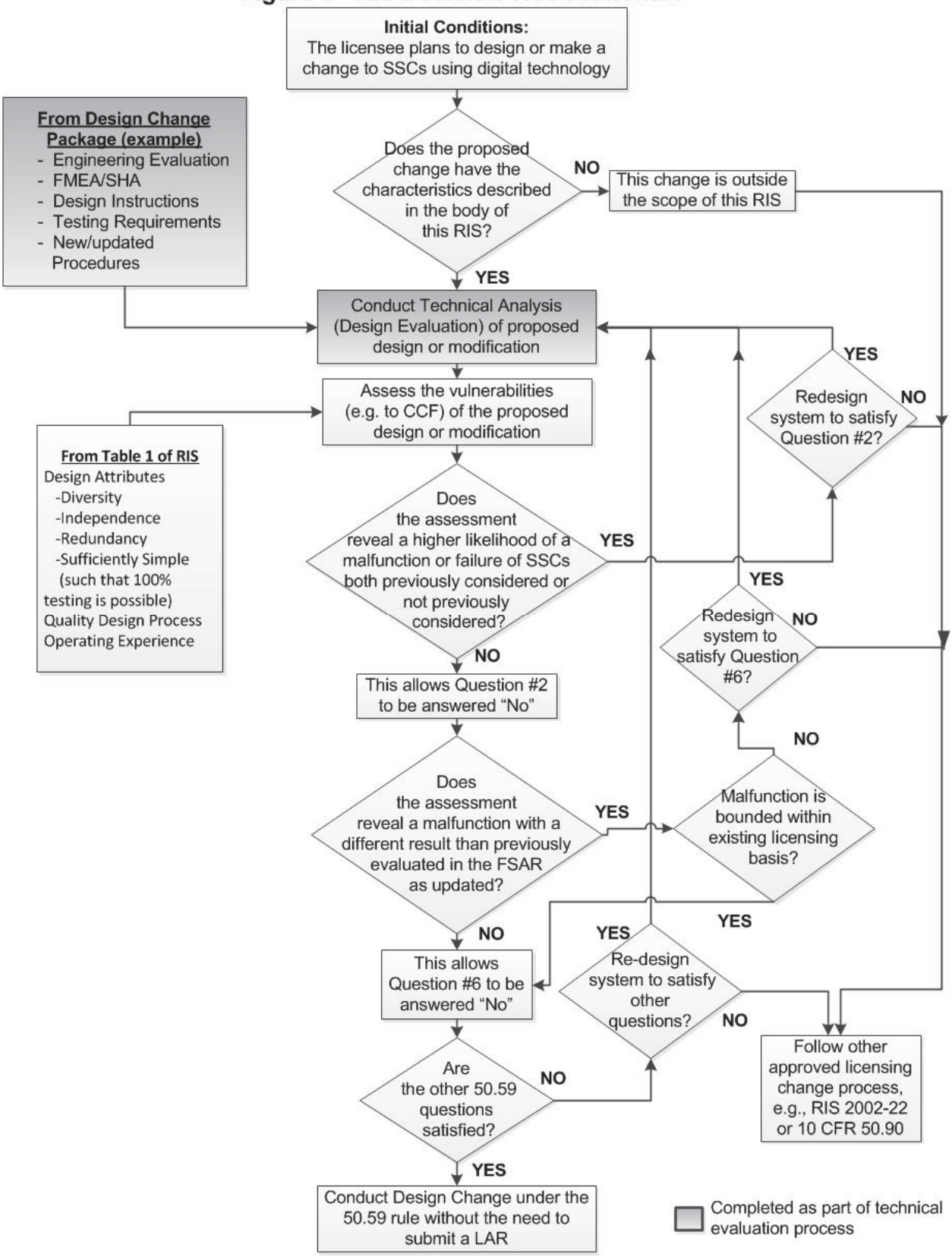
Quality standards should be documents established by consensus and approved by an accredited standards development organization that provides, for common and repeated use, rules, guidelines, or characteristics for activities or their results, aimed at the achievement of the optimum degree of order and consistency in a given context. (Example: Those published by the Institute of Electrical and Electronics Engineers (IEEE).) These are distinctly different from generally recognized guidance documents, such as guidance published by the Nuclear Energy Institute (NEI) or specifications applicable to individual plants or fleets. (Note: Quality standards describing accepted qualitative techniques do not have to be those endorsed by Regulatory Guides

3.2.3 Decision Process

The licensee has a number of options to pursue when a proposed digital I&C modification is sought. During the process of evaluating a proposed modification against the 10 CFR 50.59 evaluation criteria, it may be discovered that the proposed modification may not meet these criterion. In such a case, the licensee has the option to re-design the proposed modification until adequate qualitative evidence can be documented Re-designing a proposed modification (e.g. adding or eliminating design features or design functionality) in response to addressing potential failure vulnerabilities allows for the 50.59 performer to re-assess the proposed modification through this RIS guidance This can be an iterative process until such time that an adequate level of qualitative evidence of the reliability and dependability of the proposed modification can be used to establish, qualitatively, a low likelihood of failure, which forms the basis of the response to 10 CFR 50.59 evaluation criteria through this RIS guidance. In lieu of re-designing the proposed modification, a licensee can still pursue other avenues for performing the change.

Figure 1 of this qualitative assessment guidance provides a general overview of the types of considerations that should be made when using this guidance. Individual assessments may vary depending upon the licensee using this qualitative assessment guidance.

Figure 1 - RIS Decision Tree Flowchart



4. Qualitative Assessment Documentation

The qualitative assessment guidance describes the areas of consideration that should be documented in order to present a consistent explanation of likelihood justifications supporting technical bases for responding to 10 CFR 50.59(c)(2) evaluation criteria questions. The licensee should address each of these categories to the degree possible, as shown in Table 2. This table provides the 'process flow' that should be followed in terms of the structure of the qualitative assessment presentation as well as specific steps that licensees should address in the process.

4.1. Responsibilities of Licensees

The licensee should document the design codes and standards that were used in the development of the proposed digital I&C design modification within the design modification package. The qualitative assessment should reference the design standards used, and provide a rationale as to why those portions of design standards, as employed by experienced software and hardware engineering professionals, are considered adequate for demonstrating that a high quality component or system will result. The qualitative assessment should provide evidence that a well-defined process for project management, software design, development, implementation, verification, validation, software safety analysis, change control, and configuration control was used. The selection of the design standards (or portions thereof) to be employed should be commensurate with the level of safety significance of the modified component or system, and the possible safety consequences that may result from its failure. The design standards used need not be the same as the industry design standards referenced within NRC regulatory guides, however the licensee should be able to demonstrate why the portion of the design standard employed is considered adequate for the proposed design modification, commensurate with the level of safety significance.

4.2. Safety Significance of SSCs and Documentation of Evidence

An important consideration for documentation of evidence to address 10 CFR 50.59(c)(2) criteria is consideration of the relative safety significance of the SSC to be modified. A graded approach can be applied to accomplish this. There are numerous ways in which to correlate safety significance to level of documentation needed. The following considerations can be used as a means for determining safety significance of an SSC:

- Is the SSC(s) to be modified an event initiator?
- Is the SSC(s) to be modified part of an accident mitigation system?
- Is the SSC(s) to be modified important to maintaining barrier integrity?

Another means to correlate the level of documentation versus the safety significance of the SSC(s) to be modified is consideration of the SSC(s) role in accomplishing or maintaining critical safety functions[2] such as:

- reactivity control
- reactor core cooling
- reactor coolant system integrity
- primary reactor containment integrity
- radioactive effluent control

For modifications of greater safety significance, a higher level of technical rigor and documentation should be included with the qualitative assessment. It is the responsibility of the 10 CFR 50.59 evaluator to demonstrate that the documentation of the design basis of the proposed modification is adequate such that an independent party can arrive at the same or similar conclusions of the qualitative assessment based upon the evidence and documentation provided within, in accordance with 10 CFR 50.59(d)(1).

[2] Source: IEEE Std. 497-2002 as endorsed by RG 1.97, Revision 4

Table 2 - Qualitative Assessment Documentation Structure[3]	
Topical Area	Description
Identification	Describe the full extent of the SSC(s) to be modified—boundaries of the design change.
Step 1 - Design Function	• What is the entirety of the UFSAR design function(s) of the upgraded component(s) within the context of the plant system, subsystem, etc. • Describe what design functions were covered by the previously installed equipment, and how those same design functions will be accomplished by the modified design. Also describe any new design functions to be performed by the modified design that were not part of the original design. • Assumptions and conditions associated with the expected safety or power generation functions.
Step 2 - Failure Modes	What are the failure modes of the upgraded component(s), and are they different than the failure modes of the currently installed component(s)?
Step 3 – Results of their Failure and impact on 50.59 evaluation criterion (ii) and (iv)	In terms of existing safety analysis or in terms of an enhanced safety analysis, what are the potential safety impacts of any new postulated single failures or CCF of modified SSC(s)? Could those potential impacts already be bounded by the results of the licensing basis analyses, or would the analyses need to be revised to address it?
Step 4 - Assertions	What are the assertions being made: • The digital component is at least as reliable, dependable, etc, as the device previously installed? • The digital component(s)' likelihood of postulated CCF likelihood is significantly lower than the likelihood of the single failures considered in the UFSAR or comparable to CCFs that are not considered in the safety analyses (e.g. design flaws, maintenance errors)? ALL assertions should fully address the results of a postulated CCF of the SSC(s) to be modified and the likelihood status of postulated CCF. The qualitative assessment is not required to determine the absolute likelihood of failure.
Step 5 – Documentation of Evidence	Evidence should support each of the assertions (e.g. evidence of the 3 qualitative assessment justifications) including codes and standards applied, qualification for the environment (e.g., seismic, EMI/RFI, ambient temperature, heat contribution, etc.), as applicable. Quality Processes employed in the development (V&V processes used as evident in a traceability matrix, QA documentation, unit test and system test results, etc.,), defense-in-depth (e.g. inherent internal diversity, manual back-up capability, etc.), and Operating History (e.g., platform used in numerous applications worldwide, etc. with minimal failure history, etc.) Potential vulnerabilities and/or vectors to malfunctions (e.g. single failures and CCFs) should be identified and evidence that addresses potential vulnerabilities should be correlated to the potential vulnerabilities. The level of evidence provided should be commensurate to the safety significance of the SSC(s) to be modified.

Step 6 - Rationale	State why the assertion can be considered to be true, based on the evidence provided. Include justifications both supporting and detracting (pros and cons) so that the 10 CFR 50.59 user of the qualitative analysis has a feel for the relative magnitude of the uncertainties are associated with each claim. Provide justification supporting the use of the rationale.
Step 7 - Conclusion	Apply the results of the qualitative assessment to respond to each of the 50.59 evaluation questions.

[3] Establishes structure specifically for qualitative assessment similar to guidance provided in NEI 01-01 Appendix B.

NRC DRAFT REGULATORY ISSUE SUMMARY 2017-XX, "UPDATE TO THE NRC STAFF ENDORSEMENT ON THE USE OF EPRI/NEI JOINT TASK FORCE REPORT, "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" (REPORT PREVIOUSLY ENDORSED WITHIN RIS 2002-22) DATE: _____