NRR-DMPSPEm Resource

From: FREGONESE, Victor <vxf@nei.org>
Sent: Monday, July 10, 2017 11:30 AM
To: Morton, Wendell
Cc: Waters, Michael; Rahn, David; 'Archambo, Neil G'; AUSTGEN, Kati; HANSON, Jerud; REMER, Jason; Drake, Jason; FREGONESE, Victor
Subject: [External_Sender] RE: Upcoming RIS Meeting - Advance Discussions and Proposed Agenda
Attachments: NRC Draft Regulatory Issue Summary 2017-XX Supplement to RIS 2002-22 - NEI Feedback for Public Meeting [7-10-17].docx

Attached please find our notes and commentary to support continuing dialogue on the RIS, and to prepare for the upcoming public meeting.

We can go over these in our planning meeting on Wednesday.

These are not the official NEI comments as part of the public review process. Those will be submitted later

Vic Fregonese
Senior Project Manager
Nuclear Generation Division

Nuclear Energy Institute
1201 F Street, NW, Suite 1100
Washington, DC 20004
www.nei.org

M: 704-953-4544
E: vxf@nei.org

From: Morton, Wendell [mailto:Wendell.Morton@nrc.gov]
Sent: Thursday, July 06, 2017 4:35 PM
To: FREGONESE, Victor
Cc: Waters, Michael; Rahn, David; 'Archambo, Neil G'; AUSTGEN, Kati; HANSON, Jerud; REMER, Jason; Drake, Jason
Subject: RE: Upcoming RIS Meeting - Advance Discussions and Proposed Agenda

Hi Vic,

Attached is the word version of the draft RIS per your request. Also, please see my comments below in RED.

Wendell Morton
Electronics Engineer
Instrumentation, Controls, and Electronics Engineering Branch (ICE)
Office of New Reactors(NRO)
U.S. Nuclear Regulatory Commission
301-415-1658(Office)
301-415-5160(Fax)
Mail Stop: T07-E18M

Wendell.Morton@nrc.gov

From: FREGONESE, Victor [mailto:vxf@nei.org]
Sent: Thursday, July 06, 2017 9:49 AM
To: Holonich, Joseph <Joseph.Holonich@nrc.gov>
Cc: Waters, Michael <Michael.Waters@nrc.gov>; Morton, Wendell <Wendell.Morton@nrc.gov>; Rahn, David <David.Rahn@nrc.gov>; 'Archambo, Neil G' <Neil.Archambo@duke-energy.com>; AUSTGEN, Kati <kra@nei.org>; HANSON, Jerud <jeh@nei.org>; REMER, Jason <sjr@nei.org>; FREGONESE, Victor <vxf@nei.org>
Subject: [External_Sender] Upcoming RIS Meeting - Advance Discussions and Proposed Agenda

Hi Joe, thanks for the meeting invite for August 2 for the RIS Discussion. We look forward to continuing the dialogue during the public comment period.

I have some suggestions on the agenda, and for some advance discussions prior to the meeting:

- To facilitate the advance discussions and dialogue at the meeting on August 2, I request, if possible, that you send me a Word version of the RIS and attachment. This will be used to make it more efficient to transmit our notes and early feedback on the RIS documents. To be clear, these will not be the "official" NEI comments, but a way to continue to work collaboratively with the staff to prepare for the August 2 meeting. It will be fine to put our feedback in ADAMS as part of the meeting package. Done, please see attached. Given the time constraints we have, when do you expect to provide staff the official comments?
- If we can get the Word version in the next couple of days, I can get you the early feedback by Wednesday of next week. Assuming that happens, I would suggest a planning call on Wednesday of next week to discuss how to address the early feedback in the August 2 meeting. If we can't do this next week, then it will have to wait until the week of July 24, as both Neil and I are on vacation the week of the 17th. We can definitely schedule a planning call for Wednesday next week. I will send out a meeting scheduler.
- Prior discussions with the staff indicate that continuing with the tabletop/workshop format to discuss examples of Qualitative Assessments would be useful. We would like to discuss 2 examples during the August 2 meeting, and will come prepared to discuss a 3rd, if we have time. These will be provided in advance, and will consist of examples that are created in the framework described in the RIS and attachment. Regarding the agenda, we're in the process of starting to develop it now and should have something out next week so thanks for the early input. Regarding the examples, we want ensure that the examples you provide are representative of level of complexity and challenges industry has encountered as well as examples that are representative of the types of modifications that are taking place currently. We want to ensure the examples below meet those criterion stated, especially in light of the list of the types of SSCs that industry stated they want to be in the scope of the RIS, as presented back in April of this year I believe.
- Considering the above points, I propose the following items for the agenda on 8/2 for your consideration:
    - Early feedback on the RIS – NEI (60 minutes)
    - Tabletop Example #1 – Diesel generator voltage adjuster (re-cap and continuation from last public meeting) – NEI (60 minutes)
    - Tabletop Example #2 – Control Room Chiller Digital Controls – NEI (90 minutes)
    - Tabletop Example #3 – Main feedwater system digital valve controllers- NEI (90 minutes)

Regards,

Vic Fregonese
Senior Project Manager
Nuclear Generation Division

Nuclear Energy Institute
1201 F Street, NW, Suite 1100

Washington, DC 20004
www.nei.org

M: 704-953-4544
E: vxf@nei.org

This electronic message transmission contains information from the Nuclear Energy Institute, Inc. The information is intended solely for the use of the addressee and its use by any other person is not authorized. If you are not the intended recipient, you have received this communication in error, and any review, use, disclosure, copying or distribution of the contents of this communication is strictly prohibited. If you have received this electronic transmission in error, please notify the sender immediately by telephone or by electronic mail and permanently delete the original message. IRS Circular 230 disclosure: To ensure compliance with requirements imposed by the IRS and other taxing authorities, we inform you that any tax advice contained in this communication (including any attachments) is not intended or written to be used, and cannot be used, for the purpose of (i) avoiding penalties that may be imposed on any taxpayer or (ii) promoting, marketing or recommending to another party any transaction or matter addressed herein.

Sent through www.intermedia.com

Hearing Identifier: NRR_DMPS
Email Number: 189

Mail Envelope Properties (41207040FCA6A84984074E806C73D73EE0DB55)

Subject: [External_Sender] RE: Upcoming RIS Meeting - Advance Discussions and Proposed Agenda
Sent Date: 7/10/2017 11:30:08 AM
Received Date: 7/10/2017 11:30:15 AM
From: FREGONESE, Victor

Created By: vxf@nei.org

Recipients:
"Waters, Michael" <Michael.Waters@nrc.gov>
Tracking Status: None
"Rahn, David" <David.Rahn@nrc.gov>
Tracking Status: None
"'Archambo, Neil G'" <Neil.Archambo@duke-energy.com>
Tracking Status: None
"AUSTGEN, Kati" <kra@nei.org>
Tracking Status: None
"HANSON, Jerud" <jeh@nei.org>
Tracking Status: None
"REMER, Jason" <sjr@nei.org>
Tracking Status: None
"Drake, Jason" <Jason.Drake@nrc.gov>
Tracking Status: None
"FREGONESE, Victor" <vxf@nei.org>
Tracking Status: None
"Morton, Wendell" <Wendell.Morton@nrc.gov>
Tracking Status: None

Post Office: mbx023-e1-nj-2.exch023.domain.local

Files	**Size**	**Date & Time**
MESSAGE	7488	7/10/2017 11:30:15 AM
NRC Draft Regulatory Issue Summary 2017-XX Supplement to RIS 2002-22 - NEI Feedback for Public Meeting [7-10-17].docx	257599	

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

June 27, 2017

NRC DRAFT REGULATORY ISSUE SUMMARY 2017-XX
SUPPLEMENT TO RIS 2002-22

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," 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 Regulatory Issue Summary (RIS) 2002-22, dated November 25, 2002 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML023160044), in which 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) 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 is to clarify the NRC's endorsement of NEI 01-01 by providing additional guidance for preparing and documenting the "qualitative assessment" used to provide reasonable assurance[1] that a digital modification will exhibit a low likelihood of failure, which is a key element in 10 CFR 50.59, "Changes, tests and experiments," evaluations of whether the change requires prior NRC approval.

Commented [vxf1]: Please provide some insights on use of a different "standard" for reasonable assurance as used in this RIS, versus the broader regulatory standard.

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 1995-02, "Use of NUMARC/EPRI Report TR-102348, 'Guideline on Licensing Digital Upgrades,' in Determining the Acceptability

[1] "Reasonable assurance" appears in NEI 01-01, but as used in this RIS, means "an adequate degree of certainty" rather than the broader NRC regulatory standard.

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 and operating licenses have used this 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 Evaluations," Revision 1, dated November 2000 (ADAMS Accession No. ML003771157).

10 CFR 50.59(d)(1) 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."

NRC inspections of documentation for digital I&C plant modifications prepared by some licensees using the guidance in NEI 01-01 have uncovered inconsistencies in the performance and documentation of engineering evaluations of digital I&C modifications and inadequacies in the documentation of the technical bases supporting responses to the 10 CFR 50.59(c)(2) evaluation criteria. This RIS supplements the NRC staff's previous endorsement of the NEI 01-01 guidance by providing additional guidance for developing and documenting effective "qualitative assessments" that are used to provide reasonable assurance that a digital modification will exhibit a low likelihood of failure, which is a key element in 10 CFR 50.59 evaluations of whether a change requires prior NRC approval.

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 engaged NEI and industry representatives to improve the guidance for 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. 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). This plan, which is updated semiannually, provides a comprehensive view of NRC activities associated with improvements to the digital I&C regulatory infrastructure, including a planned schedule for completion of key regulatory infrastructure documents. In Section 5, Subsections MP#1 and MP#2 of the NRC staff's Integrated action plan (IAP), the NRC staff outlines how it plans to clarify its previous endorsement of the NEI 01-01 guidance by providing additional guidance for developing and documenting acceptable qualitative assessments in support of the performance of 10 CFR 50.59 evaluations of proposed digital I&C modifications. Making available the guidance in this RIS is described as a near-term action in the IAP to provide specific guidance for documenting effective qualitative assessments that a proposed digital I&C modification will exhibit a low likelihood of failure. The IAP also describes a longer-term plan for incorporating the guidance of this RIS into durable guidance documents that are now under development.

The NRC staff will continue to engage with stakeholders on the development of new guidance to address the identified issues and needs. The NRC staff may ultimately endorse or issue new

guidance that would supersede this RIS, however the NRC staff has not yet determined whether current efforts would eventually supersede this RIS.

SUMMARY OF ISSUE

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 NRC staff's emphasis on 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."

Specifically, this RIS provides additional guidance on what is needed to ensure that licensees adequately perform and document "qualitative assessments" used to provide reasonable assurance that a digital modification will exhibit a low likelihood of failure, which is a key element in 10 CFR 50.59 evaluations of whether a change requires prior NRC approval. For digital I&C modifications, particularly those that introduce identical software into redundant trains, divisions, or channels within a system, there may be a potential for a marginal increase in the likelihood of malfunctions, including common cause failure, occurring within the modified system. NEI 01-01 describes that for 10 CFR 50.59 evaluations, the likelihood of failure is normally demonstrated qualitatively (i.e., through reference to reasonable engineering practices or engineering judgment,) particularly for systems or components that rely on software, because there are no well-established, accepted quantitative methods to demonstrate the likelihood of failure.

Commented [NGA2]: Although this statement paraphrases NEI 01-01, Section 4.3.2, it seems to imply that digital upgrades will always result in a marginal increase in malfunction likelihood. In practice, industry has observed the opposite - that digital upgrades tend to decrease malfunction likelihood as most digital upgrades eliminate single points of vulnerability, provide for signal validation, afford internal diagnostics and alarming capabilities - to name just a few characteristics that go beyond the capabilities of their analog counterparts.

This sentence may cause confusion within industry and with regional inspectors if it is interpreted to mean that digital upgrades are expected to increase malfunction likelihood.

For digital I&C systems, reasonable assurance of low likelihood of failure is derived from a qualitative assessment of factors involving system design features, the quality of the design processes employed, and the operating history of the software and hardware used (i.e., product maturity and in-service experience). The qualitative assessment is used to record the factors and rationale and reasoning for making a determination that there is reasonable assurance that the digital I&C modification will exhibit a low likelihood of failure by considering the aggregate of these factors. The attachment to this RIS, "~~Draft~~ Qualitative Assessment Framework," provides guidance for performing and documenting this qualitative assessment.

This RIS does not change the NRC staff positions in RIS 2002-22 endorsing NEI 01-01. Specifically, RIS 2002-22 states:

> Because there is currently no acceptable way to quantitatively establish the reliability of digital systems, [NEI 01-01] gives considerable attention to the qualitative assessment of the dependability of and risk associated with I&C systems. The guidance in [NEI 01-01] identifies qualitative approaches within existing endorsed guidance with regard to software issues, including software-related common-cause failure issues, without proposing

alternatives to the existing guidance. Therefore, the guidance in [NEI 01-01] does not propose to alter, or offer less conservative guidance for, the existing licensing process for license amendment requests to implement digital replacements.

This RIS clarifies the guidance in NEI 01-01 pertaining to the performance and documentation of adequate technical evaluations and adequately documented qualitative assessments to meet the requirements of 10 CFR 50.59. The attachment to this RIS provides a framework for preparing and documenting qualitative assessments considered acceptable to serve as a technical basis supporting the responses to key 10 CFR 50.59(c)(2) evaluations.

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

NEI 01-01 supports the use of qualitative assessments, qualitative engineering judgment, and industry precedent when addressing whether the likelihood of occurrence of a malfunction would be more than minimally increased (evaluation criteria 10 CFR 50.59(c)(2)(ii)), 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 (evaluation criteria 10 CFR 50.59(c)(2)(vi)).

This RIS describes the importance of documenting how the implementation of key design attributes, quality design processes, and an evaluation of appropriate operating experience is being credited as the basis for making engineering judgments that the likelihood of malfunctions introduced by a proposed digital upgrade is low, thus ensuring that the uncertainty of qualitative assessments is sufficiently low. Such qualitative assessments are used to provide reasonable assurance that the likelihood of occurrence of potential malfunctions for proposed modifications ~~is low~~will not be more than minimally increased. Whereas the guidance in NEI 01-01 provides a "road map" to relevant standards and other sources of detailed guidance, the attachment to this RIS clarifies how the aggregate of the proposed digital I&C system design features, quality design processes, and equipment and software operating experience that are applied to the proposed design using such standards and guidance should be documented by licensees in effective qualitative assessments to support any conclusions within a 10 CFR 50.59(c)(2) evaluation that a license amendment is not needed.

Commented [NGA3]: What is meant by the statement "... ensuring that the uncertainty of qualitative assessment is sufficiently low"? Generally speaking, the qualitative assessment is used to draw the conclusion that the digital change has a low likelihood of failure. Suggest deleting this portion of the sentence as it may cause confusion.

To assist licensees in documenting adequate qualitative assessments for evaluating the 10 CFR 50.59(c)(2) criteria, the NRC staff has clarified within the attachment to this RIS its position on the content, rationale, and evaluation factors that should be addressed and evaluated within licensee-developed qualitative assessments. Specifically, the clarification within the attachment describes how such qualitative assessments should be documented to clearly demonstrate an adequate technical basis for the determination that the change does not require prior NRC staff approval.

BACKFITTING AND ISSUE FINALITY DISCUSSION

This RIS and its attachment supplements RIS 2002-22 with additional clarification about 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, and this RIS does not contain new or changed requirements or staff positions. Therefore, this RIS 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 or further address the issue finality criteria in Part 52.

***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 RIS 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. Purpose

Regulatory Issue Summary (RIS) 2002-22 provided the 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," for use as guidance for implementing and licensing digital upgrades, in a consistent, comprehensive, and predictable manner. NEI 01-01 provides design guidance in performing qualitative assessments of the dependability of digital instrumentation and control (I&C) systems.

The purpose of this attachment is to provide clarifying guidance to licensees to ensure that, if qualitative assessments are used, they are described and documented consistently, through an evaluation of all appropriate qualitative evidence available, and the use of a consistent format. Following this guidance will help licensees document qualitative assessments "in sufficient detail … that an independent third party can verify the judgements," as stated in NEI 01-01.

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

2.1 Likelihood Justifications

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 the updated final safety analysis report (UFSAR) analysis assumptions. This conclusion is used in the Title 10 of the *Code of Federal Regulations* (10 CFR) 50.59, "Changes tests and experiments," written evaluation to determine whether prior NRC approval is required prior to a digital I&C system modification.

For digital modifications under 10 CFR 50.59, licensees have experienced challenges in preparing qualitative assessments needed to support conclusions for responding to the criteria in 10 CFR 50.59(c)(2)(i), (ii), (v), and (vi).

A qualitative assessment that finds there is reasonable assurance that a digital modification will exhibit a low likelihood of failure supports the following conclusions that are necessary to a 50.59 evaluation:

- 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 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)).

As defined in NEI 01-01, Section 5.3.1, the use of the term "dependability" reflects the fact that reasonable assurance of adequate quality and low likelihood of failure is derived from a qualitative assessment of the design process and the system design features. A reliable system that performs its intended function, but exhibits other undesirable behavior is not dependable. 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.

Section 5.3.1 of NEI 01-01 also states, in part, that "reasonable assurance of adequate quality and low likelihood of failure is derived from a qualitative assessment of the design process and the system design features." Reliance on high quality development or design processes alone may not always serve as a sufficient qualitative justification. Because the qualitative assessment relies on experience and engineering knowledge, the basis for the engineering judgment and the logic used in the determination that the likelihood of failure is sufficiently low should be described and documented to the extent that another independent reviewer could reach the same or similar conclusion.

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 to determine 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 and 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 may be 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 the key element of the evaluation of criteria 10 CFR 50.59(c)(2)(i), (ii), (v) and (vi).[2]

Commented [NGA4]: It's important to note that the new digital equipment must only be as reliable/dependable as the equipment it is replacing. The likelihood of failure is relative to the equipment being replaced. The new digital equipment is not held to a higher standard than the analog (or even digital) equipment it is replacing.

The description of low likelihood of failure (i.e., the "likelihood threshold") is tailored to the criteria in 10 CFR 50.59(c)(2)(i), (ii), (v) and (vi). To make a proposed change without a license amendment, the qualitative assessment should reach a final determination that the proposed digital modification satisfies 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): The activity does not increase the likelihood of equipment failure that causes a more than minimal increase in the frequency of initiating events that lead to accidents 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 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 Part 50, Appendix B).

Commented [vxf5]: We would like to discuss why Appendix B criteria is referenced here, and the potential for mis-interpretation by end users and inspectors.

10 CFR 50.59(c)(2)(v): The activity does not create a possibility for an accident of a different type than any previously evaluated in the UFSAR because:

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

- 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): The activity does not create a possibility for a malfunction of an SSC important to safety with a different result because 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 common-cause failure (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.]

Commented [vxf6]: This term is used in several places in the document, as well as the term "significantly lower". We would like to discuss this during the upcoming meeting.

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 thresholds, the CCF alone does not indicate that a license amendment is needed to authorize the change.

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

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

2.2 Additional Considerations for 10 CFR 50.59 evaluation of criterion (c)(2)(vi)

The 10 CFR 50.59 evaluation of criterion (c)(2)(vi) can be viewed as a three-step process that stems from NEI 96-07, Revision 1, Section 4.3.6, which states: "The possible malfunctions with a different result are limited to those that are as likely to happen as those described in the UFSAR."

- Step 1 is to list "possible" malfunctions.
- Step 2 is to perform a qualitative assessment of likelihood. If there is reasonable assurance that potential failures are not as likely as those described in the UFSAR, then such failures do not merit further consideration in the 10 CFR 50.59 evaluation (i.e., the qualitative assessment provides sufficient basis that there is no malfunction with a different result.)
- Step 3 is for possible malfunctions that do not have a sufficiently low likelihood based on the qualitative assessment in Step 2, determine whether the malfunction has a different result.

For Step 1

Develop a list of "possible" malfunctions of an SSC important to safety introduced by the activity.

NEI 96-07, Revision 1, Section 3.9, states that 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.)

"Possible" malfunctions introduced by the activity as described in NEI 96-07, Revision 1, Section 4.3.6 and/or NEI 01-01, Section 4.4.6 include:

- "potential system failures…that the proposed activity could create."
- "failures of the digital device that cause the system to malfunction (i.e., not perform its design function)"
- "new components that can have failure modes different than the original components."
- "new components added that could fail in ways other than the components in the original design."
- "single failures that could previously have disabled only individual functions can now disable multiple functions"
- "the set of failures that are plausible…[that] could disable the design function"
- "a cross-tie or credible common mode failure (e.g., as a result of an analog to digital upgrade)"
- "for the purpose of the 10 CFR 50.59 evaluation, "credible" malfunctions are defined as those as likely as the malfunctions already assumed in the UFSAR."
- "malfunctions previously thought to be incredible."
- failures that "could create new results" due to (e.g., combining functions, creating new interactions with other systems, changing response time, etc.) "

Commented [vxf7]: We would like to discuss the use the term "credible malfunction" here. NEI 96-07 R1 uses "possible malfunction"

For Step 2

Perform a qualitative assessment of the likelihood of occurrence of possible malfunctions identified in Step 1 to address NEI 01-01 "The possible malfunctions with a different result are limited to those that are as likely to happen as those described in the UFSAR."

Additional guidance related to limiting possible malfunctions based on likelihood (as described NEI 96-07, Revision 1, Section 4.3.6 and NEI 01-01, Section 4.4.6) include:

- "If there is reasonable assurance that potential failures are not as likely as those described in the UFSAR, then such failures do not merit further consideration in the 10 CFR 50.59 evaluation."
- For digital modifications, particularly those that introduce software, there may be the potential marginal increase in likelihood of failure, including a single failure. For redundant systems (i.e., systems requiring the use of redundant channels), this potential marginal increase in the likelihood of failure creates a similar marginal increase in the likelihood of a common cause failure in redundant channels.
- "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)."

Commented [NGA8]: The statement identified in the bulleted item appears to be from NEI 01-01 Section 4.3.2. Where does the "including a single failure" wording come from?

Similar to a previous comment, this statement, although out of NEI 01-01, would seem to imply that digital upgrades will always increase the likelihood of failure, which has not been observed in actual practice where, in most cases, digital upgrades have been shown to decrease failure likelihood.

Also, in 50.59 it is common practice to consider the balancing of positive effects of installing the digital equipment (e.g., elimination of SPVs, signal validation, etc.) with the potential negative effects (e.g., SCCF, etc.) when arriving at the final conclusion of not more than a minimal increase in malfunction likelihood or accident frequency. The RIS does not appear to discuss using the balancing effects of the positives and negatives of digital upgrades. The RIS seems to focus only on the potential negative effects of installing digital equipment.

- The qualitative assessment "determines if there is reasonable assurance that the likelihood of failure due to software is…"sufficiently low" [which] 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 errors, calibration errors). . . "Results of this [qualitative assessment] are then used to determine whether failures due to software, including common cause failures, should be considered further in the 10 CFR 50.59 evaluation. If there is reasonable assurance that the likelihood of failure due to software is "sufficiently low,"…then the upgrade would not require prior NRC review on the basis of software common cause failures." [Importantly, this excerpt describes that, in the absence of quantitative methods, the qualitative assessment results alone are sufficient that software CCF does not need to be assumed in evaluating a "different result" for the purposes of the 10 CFR 50.59 evaluation.]

Commented [vxf9]: We would like to discuss whether the use of "software CCF" limits the use of qualitative methods to demonstrate that CCF does not have to be assumed for other types of potential common cause failures.

For Step 3

Only for possible malfunctions that do not have a sufficiently low likelihood based on the qualitative assessment in Step 2, determine whether the malfunction has a different result.

Commented [NGA10]: May need to clarify whether the different result is at the SSC level or plant level based on further discussions of this topic (next Appendix D meeting will be discussing this item).

3. Characteristics of Proposed Modifications that Produce Effective Qualitative Assessments

The qualitative assessment framework described herein may be used to develop and document the technical basis supporting a determination that a proposed digital modification satisfies each of the likelihood thresholds outlined above. The resulting qualitative assessments may then be used as part of the reasoning and rationale serving as the basis for a 10 CFR 50.59 evaluation. The NRC staff finds that proposed digital I&C upgrades and modifications having all the characteristics listed below are more suitable to and effective for qualitative assessments and thus more likely to meet the 10 CFR 50.59 evaluation criteria.

Note: The term "design functions," as used below, conforms to the definition of "design functions" as described in NEI 96-07, Revision 1.

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

   a) Do not result in 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, and
   b) Do not incorporate new shared resources (such as power supplies, controllers, and human-machine interfaces) with other system functions either explicitly credited in the final safety analysis report (FSAR) as functioning independently from other plant system functions, or implicitly assumed in the current licensing basis to be functioning independently from other plant system functions.

   "Integration," as used here, 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 and unified system or component. This would include potential upgrades to portions of safety and non-safety systems (other than reactor protection system (RPS) and engineered

Commented [NGA11]: These limitations would seem to eliminate a digital upgrade to the non-safety NSSS control system from being implemented under 50.59. If this is not the intent, may need to clarify the statement.

safeguards features (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, controllers, 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 upgrades and modifications to systems and components that do not result in reduction of any aspects of independence (or separation), single failure tolerance, or diversity credited in the FSAR; and

3. Digital I&C upgrades to facility components and systems, where a malfunction due to a design defect is precluded through simplicity (as demonstrated through 100 percent testing) or adequate internal or external diversity, or where a design defect is assumed, postulated to be triggered and demonstrated to result in no new malfunction or a malfunction that is bounded by previous FSAR analysis.

In general, the characteristics of proposed digital I&C upgrades and modifications that enable effective qualitative assessments to be prepared and documented for demonstrating a change can be implemented under 10 CFR 50.59 are those that (a) would not compromise the current design basis independence, redundancy, or diversity; (b) would not introduce a potential for a new failure that would be required to be considered within the design basis (such as introduction of new shared resources); and (c) can be shown to have such a likelihood of a design defect that would be considered to be significantly lower than that of single failures already considered in the design basis and capable of demonstration that the resulting replacement or upgrade design can tolerate the postulated triggering of that defect.

Digital I&C upgrades to facility components and systems associated with the RPS and ESF actuation systems that are not a part of the actuation logic portion of RPS and ESF actuation systems, such as changes to individual, non-shared channel inputs to RPS logic, RPS power supplies, or output actuators (relays/breakers) are acceptable for evaluation using the qualitative assessment clarification within this RIS, 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. Proposed modifications beyond these types would likely require a license amendment.

4. Qualitative Assessment

4.1. 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 overall 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, and therefore additional precautions may not be necessary. Alternatively, electrical

Commented [NGA12]: There is much industry confusion (and perhaps regional inspector confusion) over what constitutes 100% testing. Technical individuals working on the NEI/Industry DI&C teams have come to understand that any device containing software is not considered to be 100% testable. In this RIS, it would be good to elaborate on what is considered 100% testable.

Commented [NGA13]: This statement suggests that if the digital component is not 100% testable (which we've determined that any component containing software is not 100% testable), then we must assume a CCF. If this is the case, then this RIS will only work for a very limited number of digital changes. Appears to be an excerpt out of BTP 7-19 where the only options are 100% testing or diversity.

Commented [NGA14]: Bounded at the SSC level or plant level?

Commented [vxf15]: We would like to discuss and clarify methods for demonstrating what would be an acceptable way of "tolerating" the triggering of a defect.

Commented [NGA16]: This statement would seem to indicate that we must assume a design defect and then assume the design defect is triggered. If this is the intent, the RIS will likely not work for most safety related SSCs (including the safety related chiller mod). If this is not the intent, should clarify the statement.

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.

4.2. Qualitative Assessment Categories

Consistent with the guidance provided in NEI 01-01, this attachment specifies three general categories of proposed design-related characteristics (described in Table 1 below) that can be used to develop justifications that demonstrate low likelihood of failure for a proposed modification. 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 aggregate of all three categories below needs to be evaluated to demonstrate that there is reasonable assurance that the proposed modification will exhibit a low likelihood of failure such that the criteria described in Section 2 of this attachment can be addressed:

- 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 the proposed modification should prevent or limit failures from occurring or mitigate the consequences of such possible failures. The qualitative 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, design features external to the proposed modification (e.g. mechanical stops on valves) should also be considered. Attributes of the proposed modification performing within the overall channel, train, system, or plant that incorporate internal and external layers of defense against potential failures of the modified I&C system or component should be documented.

  Documentation is needed to demonstrate the proposed design will not create malfunctions with different results or initiate a different type of accident not previously analyzed in the UFSAR. Within the concept of layers of defense, acceptable justification for concluding an accident of a different type will not be initiated include the postulated new accident is only possible after a sequence of multiple unlikely independent failures. This type of justification should also be documented as part of the qualitative

assessment.~~Documentation is needed to demonstrate how the proposed design avoids 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 include that the occurrence of a postulated failure is only possible after a sequence of multiple unlikely independent failures. This type of justification should also be documented as part of the qualitative assessment.~~

- Quality Design 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.

  For the purposes of this attachment, and consistent with the guidance provided in NEI 01-01, "Quality Design Processes" means those processes employed in the development of the proposed modification that should include software development, hardware and software integration processes, hardware design, and validation and testing processes that have been incorporated into the development process.

  Note: "Quality Design Processes," as used here, does not necessarily refer to 10 CFR Part 50 Appendix B requirements. Whether the term "Quality Design Process," includes Appendix B programs depends on whether an SSC subject to Appendix B is a part of a proposed change.

- 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, operating history can be used as a means to help demonstrate that software and hardware employed in a proposed modification has 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 operating environment along with consideration of the suppliers of such equipment incorporate quality processes such as continual process improvement, incorporation of lessons learned, etc. provides further evidence of adequate reliability.

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 quality assurance (QA) program, in consideration of the safety significance of SSCs described below in Section 4.2. **(See Table 1.)**

Commented [NGA17]: These attributes may not be available or well documented for non-safety related equipment that contains software. NEI 01-01 was primarily written to evaluate changes to safety related SSCs. Quoting this paragraph within the RIS may lead some (including regional inspectors) to believe that all these attributes must be accounted for when implementing a non-safety related digital upgrade with software involved.

Commented [NGA18]: What is specifically meant by "... documented within the licensee's QA program"? Does this mean a formal qualitative assessment document must be developed and placed within the engineering change package for future retrieval?

Table 1—Qualitative Assessment Category Examples	
Categories	Acceptable Examples for Each Category
Design Attributes	• Design criteria—Diversity (if applicable), Independence, and Redundancy. • Inherent design features for software, hardware or architectural/network—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 percent testing). • Unlikely series of events—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 Design Processes	• Compliance with industry consensus standards as applicable—for non-NRC endorsed codes and standards, the licensee should provide an explanation for why use of the particular non-endorsed standard is acceptable. • Use of Appendix B vendors. If not an Appendix B vendor, the analysis should state which generally accepted industrial quality program was applied. • 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 provide a higher likelihood of resolution of potential deficiencies.

Commented [NGA19]: The RIS should not limit credit for external watchdog timers only. There are designs that have internal watchdog timers that operate independent of the software and are considered just a reliable as external watchdog timers (the digital reference adjuster used on the EDG voltage regulator project is an example of an independent internal watchdog timer). Suggest changing to "Watchdog timers that operate independent of software" or something to that effect.

Commented [vxf20]: We would like to discuss the use of 100% testing, versus other concepts, such as comprehensive, or exhaustive testing.

Commented [NGA21]: An acceptable failure state could also simply be equivalent to the failure state of the device being replaced, not necessarily to the safe state. In other words, the failure state of the new digital equipment can be the same as the failure state of the existing equipment (whether or not the failure state is considered safe).

4.2.1 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 and features are adequate.

Changes in how requirements are met need to be evaluated to ensure that they do not result in ~~a potential~~more than a minimal increase in likelihood of failure. In addition, there are some SSCs that have few applicable requirements (e.g. no diversity or redundancy requirements).

These SSCs may have been implemented in a manner (i.e., relatively independently) such that only individual SSC malfunctions or failures were considered in the UFSAR. If these individual SSCs are combined with (e.g., controlled by a common digital component) or coupled to each other (e.g., by digital communication), then the potential for ~~new~~ malfunctions with a different result ~~and~~ or accidents of a different type should be evaluated under 10 CFR 50.59.

4.2.1.1 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) is outside the scope of this RIS, and such proposed modifications should be pursued under other NRC-approved processes.

Commented [NGA22]: This paragraph does not clearly distinguish between safety related and non-safety related SSCs. Would digital communication between non-safety SSCs considered out-of-scope of this RIS? For example, a plant may have two (redundant) feedwater pumps - not for plant safety but for operational convenience. Would digital communication between the two feedwater pump controllers be out-of-scope for this RIS?

4.2.1.2 Combination of Functions

Combining functions 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 (i.e., single failures and CCF). Combined functions that can cause a plant transient, are credited for mitigating plant transients either directly or as an auxiliary support function, or are of different echelons of defense-in-depth are of greatest concern. If the qualitative assessment determines that a new type of accident or, ~~,~~ a malfunction with a ~~new~~ different result now exists due to the combination of functions, ~~or an unbounded malfunction or accident now exists due to the combining of functions creating new malfunctions, or new inter-system interactions, etc.,~~ then the licensee has the option to re-design the proposed modification to have the characteristics covered within this RIS or pursue other NRC-approved processes.

4.2.2 Quality Design Processes and Quality Standards

General Design Criterion 1 “Quality standards and records,” states:

> 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. Where generally recognized codes and standards are used, they shall be identified and evaluated 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. 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. 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.

Consistent with quality design processes as defined in Section 4.2 of this attachment, the demonstration of a defined process that incorporates the design, verification and validation, testing, etc. used in the development of a proposed modification are essential to demonstrating that the defined process (i.e., typically described within a quality standard as described in General Design Criterion 1) is a factor in the reliability and dependability of a proposed modification.

For purposes of this RIS, 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. For example, the Institute of Electrical and Electronics Engineers (IEEE) publishes consensus-based quality standards relevant to digital I&C modifications and is a generally recognized standards production organization. Quality standards used to ensure the proposed change has been developed using a quality design process do not need to be 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.

Commented [vxf23]: We would like to discuss the use of the term "quality standards" in the RIS. If the intent is to define a high quality design process, then the licensee Appendix B program should govern the activities. There is no requirement for mandatory use of any other type of quality standard for non-safety related applications.

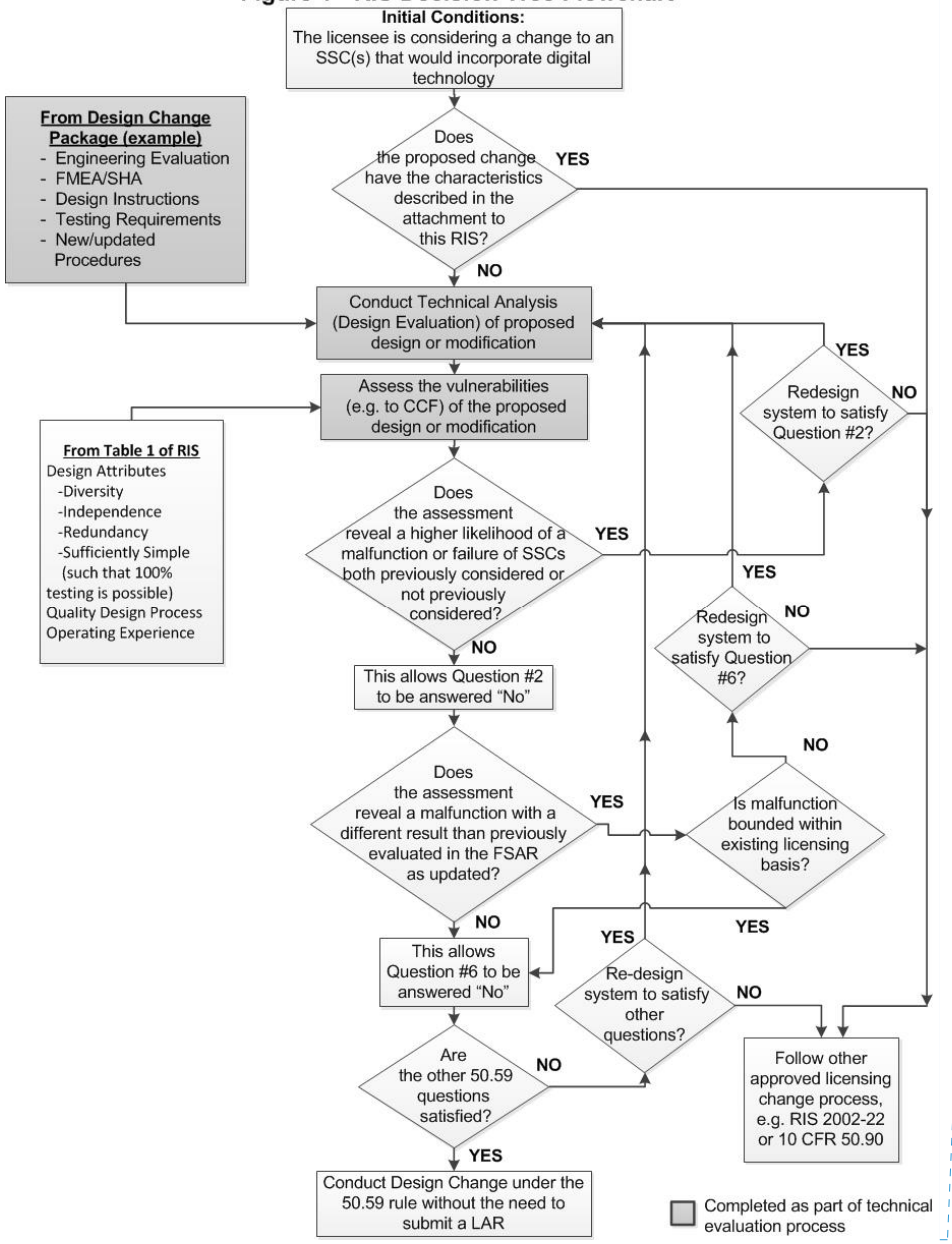
While the NRC recognizes that licensees may choose to employ non-industry consensus standards or internally-developed design standards for use with digital modifications to SSCs, for purposes of this RIS, modifications that employ industry consensus standards provide reasonable assurance of design quality incorporated in the development of a proposed modification as well as providing a more verifiable reference to an independent reviewer.

4.2.3 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, the licensee may determine 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 a design is arrived at that can be implemented without needing a license amendment. In lieu of re-designing the proposed modification, a licensee can still pursue other avenues for performing the change, i.e., a license amendment.

Figure 1 of this qualitative assessment guidance provides for the kind of process that should be engaged when using this guidance. Individual assessments may vary depending upon the licensee's individual situation using this qualitative assessment guidance.

Figure 1 - RIS Decision Tree Flowchart



Commented [NGA24]: The first decision diamond asks "Does the proposed change have the characteristics described in the attachment to this RIS? Suggest being more specific by adding a specific section number of the RIS that details the characteristics. (RIS Section 3?)

Looks like the "Yes" and "No" decisions are reversed in this diamond - if the proposed change has the characteristics described in the RIS, shouldn't we then proceed to the Technical Evaluation?

Also noted that the flowchart only addresses 50.59 Evaluations Questions 2 and 6. Questions 1 and 5 do not appear to be addressed in the flowchart.

5. Qualitative Assessment Documentation

The qualitative assessment guidance describes the areas of consideration that should be documented in 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.

5.1. 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 endorsed 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.

Commented [NGA25]: This section appears to be written for safety related software. In most cases, the evidence required in Section 5.1 would be difficult to compile for non-safety software containing COTS devices.

5.2. 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:

- Are the SSCs to be modified event initiators?
- Are the SSCs to be modified part of an accident mitigation system?
- Are the SSCs to be modified important to maintaining fission product barrier integrity?

Commented [NGA26]: Is this statement referring to accident mitigation systems that are credited in the safety (or accident) analysis? There are some non-safety systems that can be used for accident mitigation but are not credited in the safety (accident) analysis (e.g., off-site power is the preferred source of power for mitigating accidents but is not generally credited as an accident mitigator in the safety (accident) analysis). There is some confusion in the industry when it comes to defining a SSCs that are considered accident mitigators. Suggest clarifying by stating "... accident mitigation system credited in the safety analysis."

Another means to correlate the level of documentation versus the safety significance of the SSCs to be modified is consideration of the SSCs' role in accomplishing or maintaining critical safety functions[3] such as:

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

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

- 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 licensee's 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, in accordance with 10 CFR 50.59(d)(1).

Commented [vxf27]: We would like to discuss where design basis information is documented, versus where licensing basis information is documented.

Table 2—Qualitative Assessment Documentation Structure[4]

Topical Area	Description
Identification	Describe the full extent of the SSCs to be modified—boundaries of the design change.
Step 1—Design Function	• What are all of the UFSAR described design functions of the upgraded components 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. • What assumptions and conditions are associated with the expected safety or power generation functions?
Step 2—Failure Modes	What are the failure modes of the upgraded components, and are they different than the failure modes of the currently installed components?
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 SSCs? ~~Could those~~Are potential impacts already ~~be~~ bounded by ~~the~~ results described in the UFSAR ~~of the design basis analyses,~~ or would the ~~analyses~~ UFSAR need to be revised to address ~~it~~new potential impacts?
Step 4—Assertions (See Table 1)	What are the assertions being made: • The digital component is at least as reliable, dependable, etc, as the device previously installed? • The digital components' ~~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 SSCs to be modified and the likelihood status of postulated CCF. The qualitative assessment is not required to determine the absolute likelihood of failure.

Commented [NGA28]: Not sure what this statement is asking - please clarify.

Commented [vxf29]: We would like to discuss and get some clarification on what "enhanced" safety analysis means.

Commented [NGA30]: This statement implies that the licensee must assume a CCF. If this is not the case, consider re-wording or provide clarification

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

Step 5—Documentation of Evidence	Evidence should support each of the assertions (e.g. evidence of the three 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 Design Processes employed in the development (e.g., verification and validation 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 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 SSCs 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 licensee's 10 CFR 50.59 evaluator 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.

Commented [vxf31]: We would like to discuss use of this terminology and what the NRC staff thinks it means.

SUBJECT: NRC DRAFT REGULATORY ISSUE SUMMARY 2017-XX SUPPLEMENT TO RIS 2002-22 DATE: June 27, 2017

ADAMS Accession No.: Pkg: ML17123A097; RIS: ML17102B507; *concurred via email TAC No. MF9464

OFFICE	NRR/DPR/PM	NRR/DPR/PGCB/LA*	NRR/PMDA*	OE/EB*
NAME	BHarris	ELee	LHill	JPeralta (w/comment)
DATE	6/23/17	5/4/17	5/02/17	5/08/17
OFFICE	OCIO*	NRR/DE/EICB*	NRR/DE/EICB/BC*	NRO/DEIA/ICE*
NAME	DCullison	DRahn	MWaters	WMorton (DCurtis for)
DATE	5/10/17	5/11/17	5/11/17	5/11/17
OFFICE	NRO/DEIA/ICE/BC*	RES/DE/ICEEB/BC*	RES/DE/D*	NRR/DE/D*
NAME	DCurtis	IJung	BThomas	JLubinski
DATE	5/11/17	5/11/17	5/16/17	5/12/17
OFFICE	NRO/DEIA/D*	OGC*	NRR/DPR/PGCB/PM*	NRR/DPR/PGCB/LA*
NAME	RCaldwell (DCurtis for)	TCampbell	BHarris	ELee (NParker for)
DATE	5/11/17	6/23/17	6/23/17	6/26/17
OFFICE	NRR/DPR/PGCB/BC			
NAME	AGarmoe			
DATE	6/27/17			

OFFICIAL RECORD COPY