NRR-DMPSPEm Resource

From: FREGONESE, Victor <vxf@nei.org>
Sent: Wednesday, April 26, 2017 2:23 PM
To: Drake, Jason
Cc: Morton, Wendell; Rahn, David; GEIER, Stephen; REMER, Jason
Subject: [External_Sender] NEI Comments on Draft RIS and Draft Qual Assessment Guidance
Attachments: Draft_RIS_to_Clarify_RIS_2002-22_ 04-20-2017 Meeting Copy [NEI Comments 4-26].docx; Qualitative Assessment Guidance 04-20-2017 Public Meeting Copy [NEI Comments 4-26].docx

Importance: High

Jason, attached please find the NEI comments on the draft RIS and Qualitative Assessment documents that were provided by you, to NEI on April 20. *[Your email of Thu 4/20/2017 @ 7:18 AM]*

The comments have been provided in the native document format, using the "track changes" feature. (I have shortened the file name, but these are the exact documents that were attached to your email, with our edits added).

We look forward to further dialogue on these documents, and stand ready to participate in telecom's and meetings to support the FRN deadline of May 10, 2017, where the public review period will start.

Best 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

Hearing Identifier: NRR_DMPS
Email Number: 197

Mail Envelope Properties (41207040FCA6A84984074E806C73D73EDDB3CA)

Subject: [External_Sender] NEI Comments on Draft RIS and Draft Qual Assessment Guidance
Sent Date: 4/26/2017 2:22:55 PM
Received Date: 4/26/2017 2:23:15 PM
From: FREGONESE, Victor

Created By: vxf@nei.org

Recipients:
"Morton, Wendell" <Wendell.Morton@nrc.gov>
Tracking Status: None
"Rahn, David" <David.Rahn@nrc.gov>
Tracking Status: None
"GEIER, Stephen" <seg@nei.org>
Tracking Status: None
"REMER, Jason" <sjr@nei.org>
Tracking Status: None
"Drake, Jason" <Jason.Drake@nrc.gov>
Tracking Status: None

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

Files	**Size**	**Date & Time**
MESSAGE	2012	4/26/2017 2:23:15 PM
Draft_RIS_to_Clarify_RIS_2002-22_ 04-20-2017 Meeting Copy [NEI Comments 4-26].docx	71930	
Qualitative Assessment Guidance 04-20-2017 Public Meeting Copy [NEI Comments 4-26].docx	217516	

Options
Priority: High
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

July 2017

NRC REGULATORY ISSUE SUMMARY 2017-XX
UPDATE TO THE 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 BY~~WITHIN~~ 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, and all holders of, and applicants for, a power reactor combined license, standard design approval, or manufacturing license, and all applicants for a standard design certification, under 10 CFR Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants."

INTENT

The U.S. Nuclear Regulatory Commission (NRC) is issuing a clarification to the 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.") In RIS 2002-22 (ADAMS Accession Number ML023160044), the staff previously endorsed the use of the NEI 01-01 document as guidance in designing, licensing, and implementing digital upgrades and replacements in a consistent and comprehensive manner. This included providing guidance for the following activities:

a. Carry out the design and implementation process for digital replacements in a manner that ensures regulatory requirements and good engineering practices are followed.

b. Perform evaluations to comply with the requirements in 10 CFR 50.59.

c. Prepare a license amendment request (LAR) when the 10 CFR 50.59 evaluation indicates that prior NRC review is required before implementing plant changes.

d. Comply with other regulatory requirements pertaining to digital replacements in nuclear

power plants~~to instrumentation and control systems a) to ensure that digital upgrade regulatory and technical issues are adequately addressed, b) to provide criteria enabling the appropriate performance of 10 CFR 50.59 screenings and evaluations and, if necessary, c) to identify when licensees need to submit a License Amendment Request under 10 CFR 50.90 for plant upgrades using digital technology.~~

Specifically, within this RIS, the staff clarifies the applicability of its endorsement of NEI 01-01 for proposed system and component upgrades to protection systems, and to systems that support the successful operation of those systems or perform non-safety related functions. This

Commented [vxf1]: Consider adding some detail about how this RIS is to be used in conjunction with the original RIS, and what, if any content is superseded.

RIS also provides clarification of the staff's endorsement of NEI 01-01 regarding the use of criteria stated within NEI 01-01 to address the 10 CFR Part 50.59 rule, "Changes, tests, and experiments." Specifically, the staff clarifies its endorsement of the NEI 01-01 guidance for crediting deterministic and qualitative criteria for performing and documenting adequate qualitative assessments of proposed digital I&C changes within the scope of the endorsement. The documentation of ~~appropriately prepared~~ adequately performed qualitative assessments is considered an acceptable means for supporting the development of ~~adequate~~ responses to criteria required to be addressed under 10 CFR Part 50.59(c)(2)(i) through (viii). The attachment (Attachment 1) to this RIS provides clarification as to the staff's basis for continuing its endorsement of NEI 01-01, provided that the licensee documents qualitative assessments ~~are documented~~ in accordance with the guidance contained in Attachment 1. ~~therein~~.

Where potential conflicts may exist between the contents of this RIS and that of RIS 2002-22 regarding acceptable guidance for performing 10 CFR 50.59 E~~e~~valuations, the provisions within this RIS shall supersede those provided within RIS 2002-22.

It is intended that this RIS provide clarity of the staff's endorsement of NEI 01-01 for use in implementing digital I&C changes to licensed nuclear power plants that are initiated after its issuance. No backfitting is intended or approved in connection with the 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 staff review. NEI 01-01~~This report~~ replaced the original version of EPRI TR-102348, dated December 1993, which the NRC endorsed in Generic Letter (GL) 95-02, "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. In 2002, the staff issued Regulatory Issue Summary (RIS) 2002-22 to notify addressees that the NRC had reviewed NEI 01-01: "A Revision of EPRI TR-102348 To Reflect Changes to the 10 CFR 50.59 Rule," 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 staff's 2002 endorsement of NEI 01-01, holders of construction permits, standard design certifications, and operating licenses have been using this guidance, as endorsed, in support of the performance of digital ~~I&C-related~~ 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, which endorsed NEI 96-07, "Guidelines for 10 CFR 50.59 Evaluations," Revision 1, dated November 2000.

Subsequent to the issuance of the staff's 2002 endorsement of NEI 01-01, NRC inspections of plant digital ~~I&C~~ modifications performed under 10 CFR 50.59 have revealed that some

licensees have encountered difficulties in addressing the guidance and acceptance criteria within other applicable technical guidance documents while conforming to the endorsed guidance within NEI 01-01 and ~~subsequently~~ performing effective 50.59 E~~e~~valuations as required by 10 CFR 50.59(c)(2), as amended. NRC staff inspections of design modifications performed by some licensees have also revealed weaknesses in the adequacy of documentation ~~specifying~~ of the technical basis regarding licensee conclusions that the ~~evaluation~~ criteria within 10 CFR 50.59(c)(2) are being met in the proposed modernization project, and that no prior NRC staff review (such as by~~via~~ staff evaluation of a license amendment request) is required.

For example, licensees encounter difficulty addressing the staff review acceptance criteria regarding the adequacy of ~~diversity and~~ defense-in-depth and diversity (D3) analyses to address the potential for common cause failure, as outlined in versions of ~~within~~ NUREG-0800 Standard Review Plan Chapter 7, Branch Technical Position BTP 7-19, "Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems," issued after NEI 01-01 was issued ~~Revision 7~~) when they attempt to apply staff review acceptance criteria~~them~~ for use in lower safety-significant ~~I&C~~ systems/components under the 10 CFR 50.59 design change evaluation process, and subsequently provide an effective response to 10 CFR 50.59(c)(2) criteria (i) through (viii). As another example, staff inspectors have identified cases where licensee documentation supporting the technical basis for conclusions reached in 10 CFR 50.59 E~~e~~valuations is unclear as to which applicable industry codes and standards were followed, and which specific aspects of those standards provides the basis for concluding the 10 CFR 50.59 E~~e~~valuation criteria are satisfied.

Commented [vxf2]: This could be subject to interpretation. Please consider clarifying or removing.

Commented [vxf3]: This could imply that digital upgrades to systems always "screen in". Please clarify.

Section 5.2 of NEI 01-01 provides guidance regarding the need for D3 analyses to be completed for key reactor ~~protection~~ trip and engineered safety features actuation systems. Specifically, Section 5.2.1 states that a formal defense-in-depth and diversity analysis per BTP 7-19 is expected "only for substantial digital replacements of RTS and ESFAS…" …" This scope is consistent with the scope of systems addressed in BTP 7-19 when NEI 01-01 was issued Based on regulatory experience with the use of NEI 01-01, the staff has identified that the applicability of this guidance to ~~of~~ the scope of plant systems needs to be clarified. , since later versions of BTP 7-19 expanded the scope of applicability. (The staff notes that guidance for assessing the ~~diversity and~~ defense-in-depth and diversity of digital ~~I&C~~ systems/components was originally developed for use by NRC staff in their review of high safety-significant ~~I&C~~ systems/components such as reactor trip~~protection~~ systems and engineered safeguards systems in conjunction with its evaluation of license applications and amendments, rather than for use in performing design changes for less safety significant systems under 10 CFR 50.59.)

In an effort to remedy the difficulties described above, the staff, NEI, and industry representatives have been meeting to discuss these issues and are working to develop revised guidance for incorporating digital ~~I~~&C ~~systems~~related design modifications under the 10 CFR 50.59 process, and new guidance for addressing the potential for digital system ~~-~~related common cause failures. This effort is part of a broader effort to modernize the current

regulatory infrastructure to efficiently address risks associated with the introduction of digital technology for nuclear power plant applications that have potential impact on plant safety. The staff's plan for accomplishing this regulatory modernization, is outlined in the NRC "Integrated Action Plan to Modernize Digital Instrumentation and Controls Regulatory Infrastructure" (ADAMS Accession Number ML17102B307~~XXXXXXX~~), including the planned schedule for completion of key infrastructure improvements. As part of this plan, however, the staff and stakeholders have identified an immediate need for clarification of the staff's guidance for performing adequate 10 CFR 50.59 E~~e~~valuations associated with proposed digital ~~I&C~~ modernization projects ~~being implemented~~licensees are implementing under the design change process.

In this RIS, the staff ~~is~~ clarifyies~~ing~~ the applicability ~~its~~ of the previous endorsement of NEI 01-01 to reactor protection functions, and its applicability to manual control functions, and safety support systems, and non-safety systems. The staff is also clarifying its position with regard to acceptable methods for applying the guidance in NEI 01-01 to digital ~~I&C~~ modifications performed under the 10 CFR 50.59 process, in conjunction with the use of the staff's other technical guidance documents. The staff's previous endorsement is also being clarified to provide the staff's position on acceptable methods for developing and documenting qualitative assessments of the proposed digital ~~I&C~~ design change to serve as a technical basis for responding to the eight criteria that must be addressed within 10 CFR 50.59(c)(2)(i) through (viii) in order to make a change to the facility without first obtaining a license amendment under 10 CFR 50.90.

Commented [vxf4]: There does not appear to be any areas of this RIS or attachment that discuss manual control functions. Suggest defining how, or if, manual controls are to be credited in the qualitative assessment process.

Commented [vxf5]: There are some industry members who interpret that the previous guidance (RIS 2002-22) did not apply to non-safety systems. Please clarify or remove this statement.

Commented [vxf6]: If the RIS is clarifying an endorsement or position contained in other NRC technical guidance documents, please be specific and identify those areas within the RIS.

Commented [vxf7]: Industry and NRC staff should discuss further what is an "acceptable method", and level of evidence required for modifications that "screen out".

SUMMARY OF ISSUE

The revision of 10 CFR 50.59 effective on March 13, 2001, used ~~evaluation~~ criteria that are difficult to apply to software-based ~~I&C~~ systems. Therefore, the EPRI/NEI Joint Task Force included relevant supplemental guidance in developing NEI 01-01, and provided supplemental guidance on the use of NEI 96-07 for evaluating whether a proposed change to the design of the plant as described in the UFSAR using digital ~~I&C~~ technology has an impact on the plant licensing basis, and requires prior review by the NRC staff.

In its 2001to ~~-~~2002 review of NEI 01-01, the staff concluded that the document provides suitable guidance both for designing a digital ~~I&C~~ replacement and for determining whether it can be licensed and implemented under 10 CFR 50.59 without prior staff approval. Nevertheless, the staff's evaluation of the report attached to RIS 2002-22 provided statements that qualify the NRC staff's endorsement, and provided staff positions on several aspects of the design and licensing processes. In particular, the staff noted that when using the submittal (NEI 01-01) as guidance for the analysis of digital modifications of some safety-significant systems such as the reactor trip~~protection~~ system and engineered safety features actuation systems, "it is likely these digital modifications will require staff review (i.e., via a license amendment under 10 CFR 50.90) when the 10 CFR 50.59(c)(2) criteria are applied and assessed~~evaluated~~."

It is the intent of this RIS to provide further clarification of the staff's endorsement stated in RIS 2002-22 with regard to a) the endorsed scope of its applicability; b) considerations for documentation of conclusions regarding whether a digital ~~I&C~~ modification can be appropriately implemented within the 10 CFR 50.59 process; and c) clarifications to the staff's technical evaluation attached to RIS 2002-22 pertaining to documentation of qualitative assessments and other statements made.

Commented [vxf8]: Refer to previous comment on clarifying the scope of the new RIS used in conjunction with the existing RIS

Commented [vxf9]: Please be specific with respect to what "technical evaluation" is being referred to here.

Scope of Applicability of Qualitative Assessment Guidance

In Section 2.2 of the staff's evaluation of NEI 01-01 (Attachment 1 of RIS 2002-22) the staff noted that the guidance of NEI 01-01 "is intended to apply to both small and large-scale digital replacements, from the simple replacement of an individual analog meter with a microprocessor-based instrument up to the complete change out of a reactor protection system with a new, integrated digital system or replacements of mechanical or electrical equipment if the new equipment uses digital technology." In Section 3.1 of the staff's evaluation of NEI 01-01, the staff acknowledges that with regard to the replacement of complex systems, "particularly the reactor protection system (RPS) and engineered safety features actuation systems (ESFASs), there is no consensus method for determining the likelihood of software malfunctions, and system-level failure modes may exist that can have consequences different from those previously analyzed in the UFSAR. Hence, the staff believes that when using the submittal as guidance for the analysis of digital modifications of some safety-significant systems such as the RPS and ESFASs, it is likely these digital modifications will require prior staff review when 10 CFR 50.59 criteria are applied."

Commented [vxf10]: Please clarify whether the Attachment to the RIS is considered by the NRC staff to be bases, or guidance.

In this RIS, the staff is clarifying that it is the staff's expectation that the analysis and documentation of possible digital technology-related failures, including possible CCFs, within proposed modifications to the safety logic portions of all reactor trip system (RTS) ~~RPS~~ and engineered safety features initiation systems (e.g., ESFAS and other ESF actuation logic systems) should implement the analysis process outlined in NUREG 0800, Chapter 7, Branch Technical Position BTP 7-19, "Guidance for Evaluation of Diversity and Defense-In-Depth in Digital Computer-Based Instrumentation and Control Systems," and NUREG-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems." Documentation of the results of the BTP 7-19/NUREG-6303 analyses should be part of the documentation needed to support a decision as to whether prior staff review is required before the proposed modification can be implemented. However, when evaluating whether proposed digital technology changes to the non-logic portions of RPS and ESF actuation systems, and other proposed safety support systems, auxiliary systems, and non-safety systems, the guidance for adequately documenting qualitative assessments as described in the attachment to this RIS (Attachment 1) should be followed.

Commented [vxf11]: Staff comments on NEI 01-01 Appendix D have requested CCF be changed to SCCF (Software Common Cause Failure). Suggest further discussion on going forward use of "CCF" versus "SCCF", and correcting all instances in this document

Commented [vxf12]: This RIS is requiring (staff expectation) that BTP 7-19 is to be followed by licensees. The use of BTP 7-19 can be problematic for licensees performing 50.59 Evaluations. Also, BTP 7-19 refers to codes and standards that are not part of many plant licensing bases. Please consider removing or clarifying this statement. As an example, previous NRC precedent (Shearon Harris Inspection Report, dated 8-12-2013) stated in part that…*"the criteria in the BTP was intended to provide guidance to NRC staff……and not as criteria to implement digital modifications.."*

Commented [vxf13]: Please remove this requirement, or clarify the basis and necessity to perform the a D3 in accordance with NUREG 6303 in order to support the 50.59 evaluation to conclude that NRC review is required.

Commented [vxf14]: NEI and NRC staff have discussed this during recent public meetings. Perhaps some examples of what "non-logic" is referring to would be helpful to end users.

Digital ~~I&C~~ Changes Proposed under 10 CFR 50.59

NEI 01-01 contains several references to key sections within NEI 96-07, "Guidelines for 10 CFR 50.59 Evaluations," Revision 1 (November 2000), an industry guidance document that is endorsed within ~~Regulatory Guide (~~RG~~)~~ 1.187, "Guidance for Implementation of 10 CFR 50.59, Changes, Tests, and Experiments." When followed properly while assessing~~implementing~~ a proposed facility design change, NEI 96-07 provides for the use of qualitative assessments, ~~and~~ qualitative engineering judgment, and/or industry precedent when addressing whether the likelihood~~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. Guidance within NEI 96-07 states that ~~normally~~, the determination of a malfunction frequency increase is based normally upon a qualitative assessment using engineering evaluations consistent with the UFSAR analysis assumptions. However, a plant-specific accident frequency calculation or PRA may be used as one of the tools for evaluating the effects of a proposed activity in a quantitative sense. Also, "reasonable engineering practices, engineering judgment and PRA techniques, as appropriate," should be used in determining whether the likelihood~~frequency~~ of occurrence of a malfunction would more than minimally increase as a result of implementing a proposed activity. The effect of a proposed activity on the likelihood~~frequency~~ of a malfunction must be "discernable and attributable" to the proposed activity in order to exceed the "more than minimal increase" standard. This concept was endorsed in RG 1.187, along with the endorsement of the balance of the NEI 96-07, Revision 1 document.

NEI 01-01 provides a failure analysis-based and a D3 analysis-based approach to manage risk that encompasses digital-specific issues and other possible failure causes, addressing both according to their potential effects at the system level. This RIS clarifies the staff's previous endorsement regarding the need for performance of D3 evaluations of potential digital ~~I&C~~ upgrades to RPS and ESF systems to confirm adequate diversity exists, in accordance with regulatory requirements and NEI 96-07 guidance, as well as the evaluation as to whether there is any reduction in the defense-in-depth or independence either directly described or implied within the plant licensing basis, due to any changes in safety support systems, auxiliary systems, and non-safety systems. The clarified endorsement in this RIS identifies the need for documenting key design attributes and quality management measures that, when applied appropriately, could be considered ~~as~~ adequate to demonstrate a sufficient reduction in uncertainty when performing qualitative assessments of likelihood of occurrence of a potential CCF for such lower-safety significant (i.e., non-RTS~~PS~~ and non-ESF initiation system) digital I&C proposed upgrades. Whereas the guidance in NEI 01-01 provides a "road map" to relevant standards and other sources of detailed guidance, the clarified endorsement of NEI 01-01 within 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 assessed~~evaluated~~ within licensee documentation supporting any conclusions that a reduction in uncertainty could be credited.

The NRC staff expectation regarding the documentation of qualitative assessments is to be able to describe the licensee's basis (rationale) for concluding that a particular plant design, once implemented, will not result in:

Commented [vxf15]: When considering information in NEI 96-07, use of PRA is generally limited to Evaluation Question 1 - accident frequency, not to malfunction likelihood (Evaluation Question 2).

Commented [vxf16]: Considering the comment above, should this be "accident" versus "malfunction"?

Commented [vxf17]: To be consistent with NEI 96-07, consider maintaining the terms "accident frequency" and "malfunction likelihood". There appears to be mixing of these terms in this RIS.

Commented [vxf18]: This is a complex sentence that should be revised for clarity

Commented [vxf19]: See previous comment on this term.

- more than a minimal increase in the frequency of occurrence of an accident (10 CFR 50.59(c)(2)(i)), and
- more than a minimal increase in the likelihood of occurrence of a malfunction of an SSC important to safety (10 CFR 50.59(c)(2)(ii)).

Unless there is a~~n I&C~~ malfunction of the digital system/component, there can be no postulated operational occurrences or accidents that are caused by the digital system/component ~~an I&C system~~. Therefore, when responding to the criterion in 10 CFR 50.59(c)(2)(i), it is considered acceptable to base the response on the response to the criterion in 10 CFR 50.50(c)(2)(ii). Also, unless a CCF is as likely to occur as a single failure (which should already be addressed in the design), the additional contribution of a new potential CCF to malfunction likelihood~~frequency~~ should be shown to be negligible, and licensees and design certification holders should be able to demonstrate a basis for concluding there is no more than a minimal increase in the likelihood of occurrence of a malfunction.

Similarly, the NRC staff expectation regarding the documentation of qualitative assessments is to be able to describe the licensee's basis (i.e. rationale) for concluding that a particular proposed modification will not:

- create a possibility for an accident of a different type (10 CFR 50.59(c)(2)(v)), and
- create a possibility for a malfunction of an SSC important to safety with a different result (10 CFR 50.59(c)(2)(vi)).

A bounded plant-level end result is not considered a different type of accident or a malfunction with a different result. When considering and addressing~~evaluating~~ the impact of potential new CCFs that are of sufficient frequency that need to be accounted for within the plant design basis, design basis analysis methods and acceptance criteria should be used. When evaluating the impact of potential new CCFs that are of negligible frequency, existing design basis analysis methods and acceptance criteria may be used, as well as beyond design basis analysis methods (best estimate) and acceptance criteria may be used in evaluating whether the plant level effect is bounded~~ing~~.

To assist licensees in preparing acceptable qualitative assessments supporting the rationale for responding to the 10 CFR 50.59(c)(2) criteria needed to conclude whether or not prior staff evaluation is required to implement the proposed digital modification, the staff has clarified within Attachment 1 of this RIS, the staff's ~~its~~ position on the minimum content, rationale, and evaluation factors that should be addressed and assessed~~evaluated~~ within licensee-developed qualitative assessments that serve as input to developing responses to the 10 CFR 50.59 E~~e~~valuation criteria. Specifically, the clarified guidance within Attachment 1 describes the staff expectations for such qualitative assessments to document an adequate technical basis for conclusions that are made regarding the relative likelihood of failure of the proposed digital ~~I&C~~ modification, based on evidence demonstrating how adequate design measures, quality processes, layers of defense, and an evaluation of relevant operating experience were considered to contribute to such likelihood of failure.

For example, the clarified guidance in Attachment 1 identifies the need to provide adequate documentation in the modification package, which should be~~(that is then~~ referenced in the

Commented [vxf20]: Requiring the impact to be "negligible" fails to consider the case in which the additional contribution of a new potential CCF to malfunction likelihood could be "discernable," but still NOT more than minimal (as allowed by NEI 96-07, Section 4.3.2). Please consider the need to add "discernable, but NOT more than minimal criterion" (See Appendix D, Section 4.3.1 and 4.3.2).

Commented [vxf21]: If the activity increases accident frequency, malfunction likelihood, creates an accident of a different type, or a malfunction with a different result, a LAR is required. There is not further evaluation needed. It is acceptable to have a new malfunction - just not a new malfunction result. NEI and staff need to further discuss and align on the treatment of "beyond design basis" in the context of 50.59.

qualitative assessment.) as to what specific design standards were followed in the development of the proposed digital &C modification. This is to ensure that well-defined processes (as applicable, based on the safety significance of the equipment)for project management, software design, development, implementation, verification, validation, software safety analysis, change control, and configuration control were employed and are being credited in supporting the portion of the technical basis of the qualitative assessment demonstrating a high quality development process was used. These design standards need not be the specific standards endorsed in USNRC regulatory guides; however, an evaluation should be documented as to why the particular portions of the design standards areis considered to be adequate for the particular application, commensurate with the level of safety significance of the proposed modification, or its consequences of failure results.

Commented [vxf22]: The term "project management" may have different meanings to different engineers/utilities. Please clarify what is the context of "project management" as used here.

Commented [vxf23]: NEI and NRC staff should discuss the expectation of the level of documentation required to "reconcile" codes and standards. A formal line by line reconciliation may not be appropriate for many SSC upgrades. "Best Practice" may be an adequate justification.

Clarification of Other Statements in Attachment 1 of RIS 2002-22

Section 3.2.2 of the staff's evaluation of NEI 01-01 (Attachment 1 of RIS 2002-22) the staff noted that "for some relatively simple digital equipment, engineering evaluations may show that the risk of failure due to software is not significant and need not be consideredevaluated further, even in applications of high safety significance." At the time this statement was made, it was intended to refer to the sections within the staff guidance currently known as BTP 7-19, pertaining to the evaluation of simple digital equipment, such as embedded digital devices that may be found in actuating equipment. The NRC guidance at the time described simple as "the component function can be completely demonstrated by test." Subsequent revisions to In BTP 7-19 (e.g., in, Section 1.9 of the current version) incorporated a more specific states that one design attribute that is sufficient to eliminate consideration of software- based or software logic-based CCF: "Testability – A system is sufficiently simple such that every possible combination of inputs and every possible sequence of device states are tested and all outputs are verified for every case (100% tested)." Recently, a RIS 2016-05, "Embedded Digital Devices in Safety-Related Systems" was made available that addresses the use of such simple digital devices. RIS 2016-05 states that the guidance in BTP 7-19 is helpful when considering postulated CCFs in systems with components containing EDDs in equipment performing safety-related system execute features. In this RIS, the staff clarifies that an adequately documented qualitative assessment, as described in Attachment 1 to this RIS, documenting the technical and qualitative basis (rationale) for concluding that simple digital systems and devices have been adequately tested is acceptable. This qualitative rationale may credit test results for all reasonably testable combinations of input states along with a documented technical justification that any states not practical to test are not expected to ever occur for the particular application.

Section 3.2.2 of the staff's evaluation of NEI 01-01 (Attachment 1 of RIS 2002-22) also states that the 10 CFR 50.59 rule does not require licensees to document the screening if there is no change to the facility or procedures described in the UFSAR. It also states that "Appendix B of the submittal, "Outline for Documenting 10 CFR 50.59 Screens and Evaluations," provides an outline that licensees may use to document their screenings. The staff has reviewed Appendix B

Commented [vxf24]: Editorial comment on nested quotations

and concludes that it provides useful guidance for licensees and recommends its use." This RIS clarifies the statement regarding Appendix B of NEI 01-01. Specifically, the guidance in Appendix B should address the clarifications within this RIS regarding the appropriate documentation of qualitative assessments used for screening and evaluations, as described in Attachment 1 to this RIS.

Commented [vxf25]: This would be a useful area to discuss during a "tabletop" meeting, to align on expectations for using both Appendix B of NEI 01-01, and the new RIS Qualitative Assessment Guidance.

Section 3.2.3 of the 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 statement regarding Appendix A and Appendix B of NEI 01-01. Specifically, the documentation aspects described in the NEI 01-01 guidance in Appendix A and Appendix B should address the clarifications within this RIS regarding the appropriate documentation of qualitative assessments used for screening and evaluations, as described in Attachment 1 to this RIS.

Commented [vxf26]: Same comment as previous one regarding use of NEI 01-01 Appendices in conjunction with the new RIS.

Resolution of Staff Concerns Regarding Licensee Interpretations of NEI 01-01 Criteria

On November 5, 2013, the NRC issued a letter (ADAMS Accession No. ML13298A787) to NEI summarizing eleven~~11~~ NRC staff concerns regarding inconsistent interpretation of provisions within the guidance of NEI 01-01. On October 9, 2014, the NRC issued a meeting summary (ADAMS Accession No. ML14255A059) that identified a twelfth~~12th~~ concern.

Commented [vxf27]: Consider noting all 12 concerns and identifying which are addressed by this RIS, and which are not.

This section will contain the resolution of the 5 pertinent actionable staff concerns out of the 12 original concerns.

Within this RIS, the staff considers the concerns regarding adequate means for addressing the ~~evaluation~~ criteria in 10 CFR 50.59(c)(2) to be resolved for safety support systems, auxiliary systems, and non-safety systems. The remaining concerns that are not addressed here, will be addressed as part of the staff's evaluations for possible endorsement of Appendix D to NEI 96-07 addressing 10 CFR 50.59 processes, and new NEI guidance NEI 16-16, now being developed to address common cause failure of digital systems, as described within the NRC Digital I&C Integrated Action Plan, as summarized in SECY 17-XXXX. (ADAMS Accession Number ML17XXXXXXXX.)

BACKFITTING AND ISSUE FINALITY

This RIS clarifies the NRC's technical position on existing regulatory requirements related to performing digital I&C modifications under the 10 CFR 50.59 process. The NRC staff position in the RIS does not represent a new or changed position with respect to the need for applicants and licensees to perform adequate 10 CFR 50.59 evaluations, or to comply with 10 CFR 50.55a(h), "Protection and Safety Systems;" 10 CFR Part 50, Appendix A, "General Design Criteria for Nuclear Power Plants;" 10 CFR Part 50, Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants;" and other NRC regulations and guidance. Therefore, this RIS does not represent backfitting, as defined in 10 CFR 10.109(a)(1), or 10 CFR 70.76, nor is it otherwise inconsistent with any issue finality provision in 10 CFR Part 52. Therefore, the NRC did not prepare a backfit analysis for this RIS or further address the issue finality criteria in Part 52.

***FEDERAL REGISTER* NOTIFICATION**

The NRC published a notice of opportunity for public comment on this RIS in the *Federal Register* (XX FR XXXXXX) on May XX, 2017. The Commission received comments from XXXXXXXXXXXX. The staff's resolution of those comments is publicly available under ADAMS Accession No. ML17XXXXXXXX. The NRC published a notice of opportunity for public comment on the draft revised RIS in the *Federal Register* (XX FR XXXXXX) on May XX, 2017. The Commission received XX sets of comments as identified in the NRC staff's resolution of these comments in a publicly available document under ADAMS Accession No. ML17XXXXXXXX. This RIS reflects the NRC staff's consideration of these comments.

CONGRESSIONAL REVIEW ACT

The NRC has determined that this RIS is not a rule as designated by the Congressional Review Act (5 U.S.C. §§ 801-808) and, therefore, is not subject to the Act.

PAPERWORK REDUCTION ACT STATEMENT

This RIS contains and references information collection requirements that are subject to the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et seq.). These information collection requirements were approved by the Office of Management and Budget (OMB), approval numbers 3150-0035, 3150-0020, 3150-0011, 3150-0151, and 3150-0009.

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 contacts listed below or to the appropriate regional office.

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

John Lubinski, Director
Division of Engineering
Office of Nuclear Reactor Regulation

Robert Caldwell, Deputy Director
Division of Engineering Infrastructure and Advanced Reactors
Office of New Reactors

Brian Thomas, Director
Division of Engineering
Office of Nuclear Regulatory Research

Technical Contacts:

Attachment 1
RIS 2017-XX

Draft – Qualitative Assessment Framework

1 Introduction

This draft framework outlines the NRC staff's initial thoughts on clarifying guidance for the qualitative assessment process that takes into account differences in the level of evidence needed for SSCs of varying safety significance. The NRC staff recognizes that greater clarity in guidance for documenting the technical basis supporting proposed digital ~~I&C~~ modifications to SSCs of lower safety significance under 10 CFR 50.59 is needed.
The term "qualitative assessment" is referenced in both NEI 96-07 (as endorsed by RG 1.187) and NEI 01-01 (as endorsed by RIS 2002-22). For example, Section 5.3.1 of NEI 01-01 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 argument. The intent of this clarifying guidance is to enable licensees to ensure that adequate qualitative arguments are presented consistently, through an consideration~~evaluation~~ of all appropriate qualitative evidence available, and the use of a consistent format and rationale by which the evidence supports the conclusions needed to respond to the criteria within a 10 CFR 50.59 Evaluation. ~~-~~

RIS 2002-22 provided the staff's endorsement, with clarifications, of 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 in designing and implementing digital upgrades to instrumentation and control systems. The purpose of ~~Revision 1 to~~ NEI 01-01 was to assist licensees in ~~designing and implementing~~ licensing digital replacements in a consistent manner. NEI 01-01 provides guidance in performing qualitative assessments of the dependability of and risk associated with digital I&C systems. The NRC staff expects that licensees will document these ~~such~~ qualitative assessments ~~be~~ adequately, ~~documented~~ with the level of detail and topical area coverage needed to support licensing decisions, while enabling staff inspectors or other licensee reviewers of such assessments to ~~easily~~ understand the technical basis for the assessment conclusions easily.

2 Purpose

This enclosure provides clarification of the staff's previous endorsement of NEI guidance for performing and documenting qualitative assessments developed in support of performing a10 CFR 50.59 E~~e~~valuations for~~of~~ proposed digital modifications. Such qualitative assessments are needed to document the technical bases for concluding whether there is reasonable assurance that any failures or failure modes resulting from ~~due to~~ the implementation of the proposed digital modification are consistent with the UFSAR analysis assumptions at the plant level. This determination is needed because a decision must be made as to whether the proposed change meets the evaluation criteria in 10 CFR 50.59(c)(2) ~~without prior NRC staff approval, or whether~~ for a license amendment request (LAR) or the change can be implemented without NRC approval. ~~will be required.~~

Commented [vxf1]: Editorial comment - This paragraph appears to have a different font type than the remainder of the document.

Commented [vxf2]: This term is not defined in approved 50.59 guidance documents. Please remove or clarify.

Commented [vxf3]: NEI 01-01 is actually Revision 1 to the EPRI TR-102348.

The qualitative assessment is needed to support the process for making the following conclusions:

- The activity does not result in more than a minimal increase in the frequency of occurrence of an accident or the likelihood of malfunction or failure of an SSC important to safety to perform its intended design functions.
- The activity does not result in the more than minimal increase in the consequences of an accident or malfunction.
- The activity does not result in a new type of accident, or a malfunction with a different result.

2.1 For activities that introduce a potential CCF that meets the above conditions, the CCF alone would not require the change to be approved under 10 CFR50.90 through a LAR.

2.2 For activities that introduce a potential CCF that do not meet the above conditions, the CCF would need to become part of the licensing basis; a LAR ~~licensee amendment~~ would be required under~~. (via~~ 10 CFR 50.90~~.)~~.

2.3 This qualitative assessment clarification is intended to augment~~clarify~~, rather than replace the guidance provided for qualitative assessments that are described in NEI 01-01, Sections 4.4 , 5.1, and 5.3 as well as Appendix A~~. (Item~~s Nos. 2(i) & 6(b)~~)~~.

3 Qualitative Assessment

3.1 Scope

The qualitative assessment process may be applied to any proposed digital ~~I&C~~ plant modification~~s~~ to safety and non-safety systems. However, at this time, it is not intended for this RIS to apply to reactor trip~~protection~~ or essential safety feature initiation functions. Consistent with the staff's endorsement of NEI 01-01 in RIS 2002-22, it is likely that ~~when applying NEI 01-01 for completing the~~ the10 CFR 50.59 E~~e~~valuation ~~process~~ defined in NEI 01-01 will require a LAR ~~for proposed~~to implement significant changes to reactor trip ~~protection~~ and engineered safeguards initiation systems~~., it will be found that a license amendment request will be necessary to make the change~~.

3.2 "Quantitative vs. Qualitative"

A quantitative assessment involves the use of numbers in measurements, comparisons, or calculations. A qualitative assessment is any other assessment that is not quantitative. For example, an electrical independence requirement can be demonstrated, quantitatively, by comparing the capacity of an electrical isolation device with anticipated challenges to it. Alternatively, an electrical independence requirement can be demonstrated qualitatively by showing that the independent channels of equipment have no shared common components and have no electrical connections between them.

Commented [vxf4]: Staff comments on NEI 01-01 Appendix D have requested CCF be changed to SCCF (Software Common Cause Failure). Suggest further discussion on going forward use of "CCF" versus "SCCF", and correcting all instances in this document

Commented [vxf5]: Calling these 2 sections of Appendix A out may imply limiting the scope to just software, but many upgrades are more than software. Consider just referring to the appropriate NEI 01-01 sections and Appendix A.

Commented [vxf6]: The RIS discusses logic functions. Please clarify this area to be consistent.

Commented [vxf7]: Clarification may be required for the use of "significant" here. The intent would be to remain consistent with the logic functions addressed elsewhere in the RIS and Attachment. Also, some digital to digital, or other module/piece part RTS or ESFAS changes may be desired to be done under 50.59, and addressed appropriately in the Qualitative Assessment.

3.3 Qualitative Argument Cornerstones

This Qualitative Assessment clarification highlights four general categories of proposed design-related characteristics, each of which needs to be assessed~~evaluated~~ to formulate effective qualitative arguments deemed sufficient to address the three questions posed in the "Purpose" section above. ~~The staff finds that an~~An evaluation of the degree to which each category of design characteristic has been addressed and weighed collectively in the design is adequate to support arguments within acceptable technical bases for responding to the 50.59(c)(2) criteria.~~evaluation questions~~. These areas should be assessed~~evaluated~~ , as applicable, in conjunction with the questions provided in NEI 01-01, Appendix A. Those four general categories are:

- Design Attributes of the proposed modification that serve to prevent or limit failures from occurring, or that mitigate the consequences of such possible failures. The assessment should document and describe e~~E~~vidence of design attributes supporting arguments for the high reliability and dependability of the proposed modification ~~should be described~~.

- Quality Processes employed in the development of the proposed modification, including software development, hardware and software integration processes, hardware design, and validation and testing processes that have been incorporated into the development process.

- Defense in Depth: Must be documented and show e~~E~~vidence that the proposed design incorporates both internal and external layers of defense against potential failures of the modified I&C system or component. The design must respond appropriately to avoid generating ~~that could result in~~ 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 in the initiation of new AOOs or PAs that have not been previously analyzed.

- Operating Experience: must be documented to show ~~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, deficiency and failure tracking and disposition, etc.

These categories are not mutually exclusive and may overlap in certain areas. Adequate qualitative arguments for systems of varying safety significance should address the degree to which the proposed modification has addressed each of the above categories. ~~It's the~~The staff's expect~~sation~~ the evaluation will address ~~that~~each ~~ALL~~ of these categories ~~be addressed~~ to the degree possible. **See Table 1**.

Table 1 - Qualitative Argument Topical Areas

Commented [vxf8]: Consider whether this should be measured against the 50.59 criterion of "result in more than a minimal increase in the frequency of occurrence of an accident previously evaluated in the final safety analysis report"

Commented [vxf9]: Consider clarification somewhere in the document that if the activity could result in a new AOO or PA that has not been previously analyzed (this would be an accident of a different type), Evaluation Question 5 would be answered YES and a LAR would be required to implement

Topical Area	Description
Design Attributes	• Design Criteria – For example: Diversity (if applicable), Independence, Redundancy • Inherent Design Features for software, hardware or architectural/network – For example: external watchdog timers, isolation devices, segmentation, self-testing and self-diagnostic features • Non-concurrent triggers • Sufficiently Simple (i.e. enabling comprehensive~~100%~~ testing) • Unlikely series of events – For example, the evaluation of a given DI&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	• Use of~~Compliance~~ ~~with~~ industry codes and standards - This includes those industry codes and standards cited within the Design and Licensing Basis and other NRC-endorsed industry codes and standards where practical for the design and application. ~~It is the expectation that for~~ Where non-NRC endorsed codes and standards are applied to the design, 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, temperature, humidity, etc.) • Development Process rigor
Defense-In-Depth	• Coping measures • Availability of operator intervention capabilities independent of the potential CCF, administrative controls, and sufficient time to respond • Physical restrictions external to the DI&C modification (e.g. mechanical restrictions on control valve movements, pump/turbine/vfd speed limits, rod control interlocks, etc.)
Operating Experience	• Wide range of operating history • 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.

Commented [vxf10]: Please consider adding a statement that makes it clear that these are examples of design measures that could be taken - the list is not a "checklist" whereby all of the listed items must be incorporated into the design.

Commented [vxf11]: NEI and staff need to discuss further how to adequately describe and bound this topic to ensure it is not open ended and subject to interpretation later.

Commented [vxf12]: Please define 100% testing. Suggested definition is:
"All reasonably testable combinations of input states along with a documented technical justification that any states not practical to test are not expected to ever occur for the particular application."

Commented [vxf13]: Please consider that BTP 7-19 at the time NEI 01-01 was issued described simple as "the component function can be completely demonstrated by test." Later versions introduced the 100% testability with all the qualifying statements.

Commented [vxf14]: "Use" would be a better choice of wording. This was discussed in the recent public meeting. "Compliance" could drive to literal compliance and all the explanations for what is not met, versus documenting the application of what codes and standards were considered in the development of the design.

Commented [vxf15]: Please consider incorporating the approach in the RIS, which states:
an evaluation should be documented as to why the particular design standards are considered to be adequate for the particular application, commensurate with the level of safety significance of the proposed modification, or its consequences of failure.

Commented [vxf16]: Please clarify what the intent is here. ("sufficient") This statement could imply that critical operator actions apply.

3.3.1 Design Attributes versus Quality Process

Both "Design Attributes" and "Quality Process" are needed because to some degree each~~they~~ address~~es~~ different aspects, and to some degree ~~they~~ complement each other. For example, the surface of a weld should be appropriately cleaned (a Design Attribute) before the welding is performed, in part, to ensure a proper weld. It is generally not possible to tell, from inspecting the weld after it is completed, that the surfaces were properly cleaned. Therefore, Quality

Processes ensure and document: the welder is trained in the appropriate cleaning processes, and in-process inspections are performed to ensure the weld surfaces are cleaned.

3.3.2 Design Attributes to Eliminate Consideration of CCF

Many system design and testing attributes, procedures, and practices can contribute to significantly reducing the probability of CCF. ~~However,~~ NUREG-0800 Chapter 7, Branch Technical Position No. 7-19 ~~only~~ recognizes two design attributes as sufficient to eliminate consideration of software- based or programmable ~~software~~ logic- based CCF: Diversity or Testability. However, if CCF is considered in a larger context (i.e., software- based or ~~software~~ programmable logic- based CCFs are not the only types of CCFs), then there are many regulatory requirements to address potential CCFs, and thereby eliminate CCFs~~them~~ from further consideration. As a result, any relaxations in how these requirements are met, are "adverse" in a 50.59 Screen ~~should screen in~~ (and thus ~~i.e.,~~ require a ~~full~~ 50.59 E~~e~~valuation). Changes in how requirements are met need to be assessed~~evaluated~~ to ensure they do not result in a need for a license amendment. 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 (e.g., by digital communication), then the new malfunction(s) and/or accident(s) must be reviewed using the 10 CFR 50.59 process ~~evaluated under 50.59~~. NRC approved qualitative and/or quantitative methods can be used to evaluate attributes of the design to determine whether a license amendment may be required:

- Digital Communications: The introduction of digital communication (between redundancies, levels of defense, or between different safety classifications) that does not meet NRC- endorsed guidance for communications independence should be reviewed and approved under a LAR processed under 10 CFR 50.90.

- Combination of Functions: The combination of functions (that (i) can cause an AOO or PA (e.g., for non-safety-related systems, combining the functions of the feedwater control system with the functions of the turbine control system), ~~a plant transient~~, (ii) are credited for mitigating plant transients either directly or as an auxiliary support function, or (iii) are of different layers of defense) is "adverse" in a 50.59 Screen (i.e., requires a 50.59 Evaluation) ~~should be evaluated under 50.59~~. If the 50.59 E~~e~~valuation determines that: (A) a new type of accident, (B) a malfunction with a new result, or (C) an unbounded malfunction or accident now exists, then a LAR is required under 10 CFR 50.90.~~-~~

- Defense-in-depth: Defense-in-depth is an element of the NRC's safety philosophy that employs successive compensatory measures to prevent accidents or mitigate damage if a malfunction, accident, or naturally caused event occurs at a nuclear facility. The defense-in-depth philosophy has traditionally been applied in plant design and operation to provide multiple means to accomplish safety functions and prevent the release of

Commented [vxf17]: Consider using a "digital example" here in lieu of a "special process" like welding.

Commented [vxf18]: Please consider that the NRC guidance at the time NEI 01-01 was issued described simple as "the component function can be completely demonstrated by test." Later versions introduced the 100% testability with all the qualifying statements.

Commented [vxf19]: Please clarify. It might be more appropriate to use "design attributes" rather than "regulatory requirements"

Commented [vxf20]: Provide additional discussion regarding the phrase "relatively independently" to more fully explain its meaning.

Commented [vxf21]: Please clarify what is meant by endorsed guidance. RG 1.152 R3 states that IEEE Std 7-4.3.2-2003 Annex E, "Communication Independence," has not received NRC endorsement because it provides insufficient guidance.

radioactive material. Defense in Depth~~It~~ continues to be an effective way to account for uncertainties in equipment and human performance and, in particular, to account for the potential for unknown and unforeseen failure mechanisms or phenomena that, because they are unknown or unforeseen, are not reflected in either the PRA or traditional engineering analyses. The SRM on SECY-98-144, "White Paper on Risk-Informed and Performance-Based Regulation," provides additional information on defense-in-depth as an element of the NRC's safety philosophy.

Appendix A, "General Design Criteria for Nuclear Power Plants," to Title 10 of the Code of Federal Regulations (10 CFR) Part 50, "Domestic Licensing of Production and Utilization Facilities," was first promulgated in 1971 and reflects the defense-in-depth principles, although Appendix A does not explicitly refer to defense-in-depth. A balance among accident prevention, accident mitigation, and limiting accident consequences is basic to the general design criteria. Specific requirements in the general design criteria exist for independence, redundancy, (often times achieved by imposing the requirement to withstand a "single failure).and diversity. ~~(oftentimes achieved by imposing the requirement to withstand a "single failure)."~~ The general design criteria also require a level of quality commensurate with the safety functions of structures, systems, and components and require the capability for inspection and testing.

Both RG 1.174 Rev. 3 and BTP 7-19 contain criteria for determining whether adequate Defense-in-Depth has been maintained. A failure to meet either of these criteria should be reviewed and approved through a LAR under ~~a~~ 10 CFR 50.90. That is, a failure to maintain adequate defense in depth is considered to violate a criteria that is applicable to both evaluation questions 1 and~~&~~2:

> "Although this criterion allows minimal increases, licensees must still meet applicable regulatory requirements and other acceptance criteria to which they are committed (such as, contained in regulatory guides and nationally recognized industry consensus standards, e.g., the ASME B&PV Code and IEEE standards). Further, departures from the design, fabrication, construction, testing and performance standards as outlined in the General Design Criteria (Appendix A to Part 50) are not compatible with a "no more than minimal increase" standard."

Commented [vxf22]: Please clarify the applicability of RG 1.174. Industry interpretation is that RG 1.174 would apply to license amendments with a quantitative risk-informed basis. The RIS focus is on the use of qualitative assessments.

Commented [vxf23]: The draft RIS speaks of BTP 7-19 D3 criteria with respect to RPS/ESFAS modifications. The discussion here seems to suggest it be applied to all digital mods and if it cannot be met then a license amendment is needed. Please clarify this.

3.3.3 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 features of each design must be reviewed against the applicable 10 CFR 50.59(c)(2)~~50.59~~ criteria. This is in addition to the general considerations listed above.

3.3.4 Regarding codes and standards

Design attributes credited for meeting ~~any criteria~~ industry codes and standards criteria must be stated~~stipulated~~ and documented. ~~as being achieved~~

~~(per GDC 1 –~~ For those stations committed to GDC 1, Quality Standards and Records need to align with this criteria.~~):~~

(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."

The term "quality standards" is sometimes a source of confusion. Some understand this term to mean "codes and standards;" however, this interpretation would render the first clause of the second sentence irrelevant. A better interpretation of the term would be: "specified criteria." It is understood that not everything important to safety has been designed according to a generally recognized code or standard.

Commented [vxf24]: In order to avoid any ambiguity, this is an area that warrants further discussion, similar to the to the topic of technical codes and standards that NEI and NRC staff had in the last public meeting.

(2) "Where generally recognized codes and standards are used, they shall be identified and assessed~~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."

This sentence allows the use of "generally recognized codes and standards," when appropriate instead of requiring application specific specifications 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.

(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 part of an Appendix B quality assurance 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."

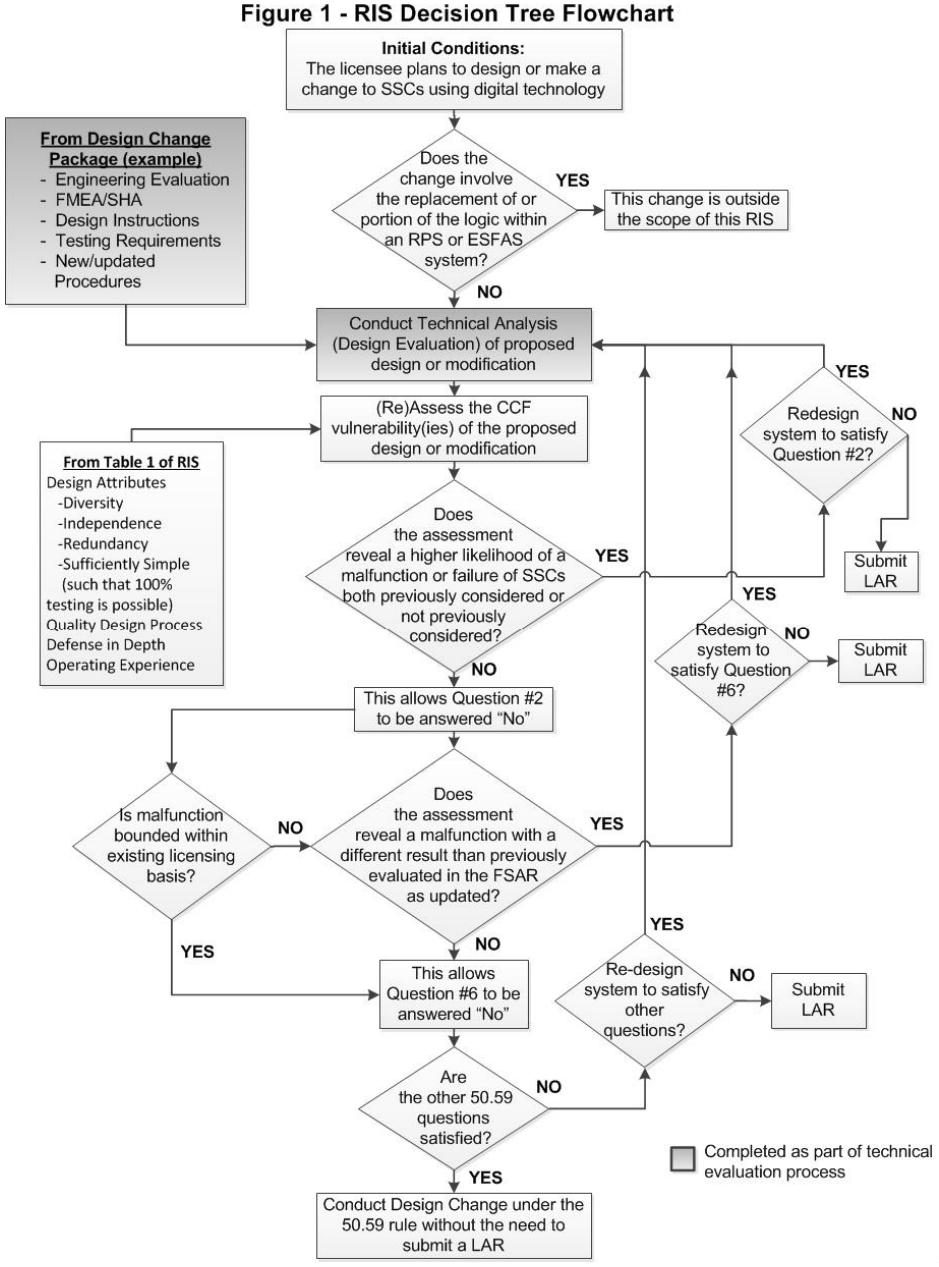
The sentence requires documentation for important to safety equipment that is not part of an Appendix B QA program.

Commented [vxf25]: More discussion on this interpretation is required to ensure it is clear on the level of documentation that would be required to support digital upgrades to non-safety related equipment.

3.3.5 Decision Process

Figure 1 of this qualitative assessment guidance provides a general overview of the types of considerations that should be made when using this guidance to address NEI 01-01 Appendix A (Items Nos. 2(i) & 6(b)). Individual assessments may vary depending upon the licensee using this qualitative assessment guidance.

Figure 1 - RIS Decision Tree Flowchart



Commented [vxf26]: There is no box for 50.59 Question #6.

Commented [vxf27]: Many of the "rectangles" on the flow chart do not have a "yes" or "no". For instance, the box that contains *"This allows Question #2 to be answered NO*". Please clarify this in the flowchart.

Commented [vxf28]: Please refer to previous comment on the 100% testability in Table 1.

Commented [vxf29]: Please clarify what the purpose of the decision block that states:
"Is malfunction bounded within the existing licensing basis?"

4 Qualitative Assessment Documentation

The qualitative assessment guidance ~~also~~ describes the areas of consideration that should be documented in order to present a consistent explanation of likelihood arguments supporting technical bases for responding to 10 CFR 50.59(c)(2) criteria ~~50.59 evaluation~~ questions. ~~It's the~~ The staff~~'s~~ expect~~sation~~ that the licensee will address each~~ALL~~ of these categories ~~be addressed~~ to the degree possible, as shown in. ~~See~~ **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 the licensee should ~~be~~ address~~ed~~ in the process.

4.1 Responsibilities of License Holders

~~It is critical that the~~ The licensee~~'s~~ ~~document in the~~ design modification package should document the design codes and standards that were used in the development of the ~~proposed~~ digital I&C design modification. The qualitative assessment should~~will~~ reference the design standards used, and provide a rationale as to why the portions of those 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, as evidenced by the fact 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. They need not be the same as the industry design standards referenced within USNRC 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 [vxf30]: More discussion is needed to clarify the extent of what is considered "adequate" for non-safety related systems, where it is unlikely to be significant use of IEEE software or other software safety analyses.

Commented [vxf31]: "Project management" may have a different definition to a licensee than the intended meaning used here. Need to clarify the meaning of "project management" when used in the context presented here.

4.2 Safety Significance of SSCs and Documentation of Evidence

As stated previously, an important consideration for documentation of evidence to address 10 CFR 50.59(c)(2) ~~50.59 evaluation~~ criteria is consideration of the relative safety significance of the SSC to be modified and a graded approach can be utilized to this end. There are numerous ways in which to correlate safety significance to level of documentation needed. Some considerations can include, but are not limited to, the following:

- 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?

Commented [vxf32]: Please clarify this bullet as to whether it is meant that SSC to be modified is the direct cause of a previously analyzed AOO, or something else.

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[1] such as:

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

- Reactivity control
- Reactor core cooling
- Reactor coolant system integrity
- Primary reactor containment integrity
- Radioactive effluent control

It is the responsibility of the 10 CFR 50.59 practitioner ~~50.59 evaluator~~ to demonstrate that the documentation of the design basis of the proposed modification is adequate based upon the safety significance of the SSC(s) to be modified and that this portion of the analysis is captured within the10 CFR 50.59 Eevaluation.

Table 2 - Qualitative Assessment Documentation Structure[2]	
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	In terms of existing safety analysis or in terms of an enhanced safety analysis, what are the consequences of any postulated single failures or CCF of modified SSC(s)?
Step 4 - Assertions	What are the assertions being made: • The digital component is at least as reliable, dependable, etc, as the device previously installed? • ~~Its~~ 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 ~~will not~~ is not required to determine the absolute probability ~~likelihood~~ of failure.

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

Commented [vxf33]: Please clarify whether this it referring to direct reactivity control, like rods or boration/dilution, or some other secondary effects that eventually will feedback to reactivity.

Commented [vxf34]: Please clarify whether this bullet is referring to Post-accident, or non-safety radwaste systems

Commented [vxf35]: Please consider an expanded discussion somewhere in the document to clarify that if it is concluded that CCF is not credible, whether the licensee still needs to assume a CCF and evaluate the results of failure.

Step 5 – Documentation of Evidence	Evidence should support each of the assertions (e.g. evidence of the 4 qualitative assessment arguments) including codes and standards applied, qualification for the environment (e.g., seismic, EMI/RFI, ambient temperature, humidity, 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.) 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 arguments 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.

Commented [vxf36]: Please consider clarification somewhere in this document about the applicability of this criteria to many modifications, such as component level, where the criteria may be too prescriptive.