NRR-DMPSPEm Resource

From: Ken Scarola <KenScarola@NuclearAutomation.com>
Sent: Friday, April 21, 2017 1:10 PM
To: Drake, Jason
Cc: Rahn, David; Holonich, Joseph; Morton, Wendell
Subject: [External_Sender] Recommendations and Comments on Staff Documents Issued in Conjunction with April 20, 2017 Public Meeting on CCF RIS
Attachments: Draft_RIS_to_Clarify_RIS_2002-22_Endorsement_of_NEI_01-01 for Public Meeting on 04-20-2017 Change Accepted_KS.docx; Qualitative Assessment Guidance for NEI 01-01 _rev1 Changes Accepted for use with 04-20-2017 Public Meeting --Changes Accepted_KS.docx

Jason,
I'm sending the files attached for Staff consideration regarding the documents made public by the staff for use in conjunction with the NRC public meeting held April 20, 2017.

There are two attachments:

1. My comments on the "Draft_RIS_to_Clarify_RIS_2002-22_Endorsement_of_NEI_01-01 for Public Meeting on 04-20-2017 Change Accepted".
2. My comments on the "Qualitative Assessment Guidance for NEI 01-01_rev1 Changes Accepted for use with 04-20-2017 Public Meeting --Changes Accepted".

In addition, in the MOP digital replacement example presented at the meeting, the attributes of low likelihood of a defect and divisional independence are used to conclude that a CCF is as unlikely as other potential sources of CCF, such as maintenance or calibration errors that are not considered in the FSAR (i.e., in essence the conclusion is that a CCF is not credible for the MOP application). But the SRM to SECY 93-087 uses these same two attributes (one qualitative, one deterministic) to conclude only that a CCF is sufficiently unlikely to be analyzed as a beyond design basis event, not to conclude that a CCF is not credible. I agree with the SRM to SECY 93-087, and maintain that to reach a CCF not credible conclusion additional deterministic design attributes are required, such as configuration differences to achieve non-concurrent triggers. What is the technical basis for changing the Staff's policy on this issue, and can a policy change be made in a RIS?

Thank you for considering this input for the RIS on CCF. I would be happy to discuss any of these comments.

Ken

_____

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

Hearing Identifier: NRR_DMPS
Email Number: 201

Mail Envelope Properties (01c601d2bac2$2f1b0f50$8d512df0$)

Subject: [External_Sender] Recommendations and Comments on Staff Documents Issued in Conjunction with April 20, 2017 Public Meeting on CCF RIS
Sent Date: 4/21/2017 1:10:27 PM
Received Date: 4/21/2017 1:11:17 PM
From: Ken Scarola

Created By: KenScarola@NuclearAutomation.com

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

Post Office: NuclearAutomation.com

Files	**Size**	**Date & Time**
MESSAGE	1757	4/21/2017 1:11:17 PM
Draft_RIS_to_Clarify_RIS_2002-22_Endorsement_of_NEI_01-01 for Public Meeting on 04-20-2017 Change Accepted_KS.docx	60432	
Qualitative Assessment Guidance for NEI 01-01_rev1 Changes Accepted for use with 04-20-2017 Public Meeting --Changes Accepted_KS.docx	206374	

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

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 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 and implementing digital upgrades 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

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 adequate ~~qualitative~~ [from the previous phrase it should be clear that NEI 01-01 requires both deterministic and qualitative assessments; qualitative assessments alone are not sufficient.] assessments of proposed digital I&C changes within the scope of the endorsement. The documentation of appropriately prepared ~~qualitative~~ digital I&C change 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 digital I&C change~~qualitative~~ assessments are documented in accordance with the guidance contained 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 evaluations, 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. 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 evaluations as required by 10 CFR 50.59, as amended. NRC staff inspections of design modifications performed by some licensees have also revealed weaknesses in the adequacy of documentation specifying the technical basis regarding licensee conclusions that the evaluation criteria within 10 CFR 50.59 are being met in the proposed modernization project, and that no prior NRC staff review (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 (D3) analyses to address the potential for common cause failure, as outlined 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," Revision 7) when they attempt to apply them for use in lower safety-significant I&C systems 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 evaluations 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 evaluation criteria are satisfied.

Section 5.2 of NEI 01-01 provides guidance regarding the need for D3 analyses to be completed for key reactor protection 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…" 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. (The staff notes that guidance for assessing the diversity and defense-in-depth of digital I&C systems was ~~originally~~ [the original scope of BTP 7-19 is irrelevant, because the scope has now been expanded to encompass all safety systems] developed for use by NRC staff in their review of ~~high safety-significant~~safety I&C systems ~~such as reactor 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 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 ML17XXXXXXX), 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 evaluations associated with proposed digital I&C modernization projects being implemented under the design change process.

In this RIS, the staff is clarifying the applicability its previous endorsement of NEI 01-01 to automatic and manual functions [applies to all of the following] for reactor protection ~~functions~~, ~~and its applicability to manual control~~engineered safety features ~~functions~~, 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.

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 using digital I&C technology has an impact on the plant licensing basis, and requires prior review by the NRC staff.

In its 2001-2002 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 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 as guidance for the analysis of digital modifications of some safety-significant systems such as the reactor 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 criteria are applied and evaluated." [I agree RIS 2002-22 said that, but there is actually nothing in the actual NEI 01-01 evaluation process that distinguishes safety significant systems from other safety systems of less safety significance; therefore, there is nothing in NEI 01-01 that would result in this conclusion.]

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 digital I&C change~~qualitative~~ assessments and other statements made.

Scope of Applicability of Digital I&C Change**~~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 ESFAS~~s~~, it is likely these digital modifications will require prior staff review when 10 CFR 50.59 criteria are applied."

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~~any portions [There is no technical basis to limit this to safety logic, because all portions of these systems are safety significant and all portions may have CCF susceptibilities (there is no way of knowing how susceptible a function is to CCF without a documented analysis).] of all RPS and engineered safety features ~~initiation~~ systems, ~~(e.g., ESFAS and other ESF actuation logic systems)~~from sensors to controlled plant components, should implement the CCF vulnerability analysis process, and for any CCF vulnerabilities should implement the AOO and PA 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." For clarity, this analysis is applicable to any equipment that is directly credited in the plant's accident analyses for accident mitigation, and any equipment that could directly prevent the credited equipment from performing its safety function (e.g., an ESF load sequencer that can block ESF actuation [for many plants sequencers can block ESF actuation during LOOP and non-LOOP conditions]). 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~~license amendment request [As written, this says that if you follow BTP 7-19 and demonstrate acceptable best estimate results, you can replace the RPS/ESF under 50.59. That is acceptable to me, but is that really what you want? I thought you were trying to limit the scope of this RIS.]. 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, can be implemented under 50.59, the guidance for adequately documenting digital I&C change~~qualitative~~ assessments as described in the attachment to this RIS (Attachment 1) should be followed [I really see very little difference between the process you have described in Attachment 1 and BTP 7-19. Both require a CCF vulnerability assessment, and for credible CCFs both require a malfunction results analysis. The only difference I see, is that you are drawing the line on which mods can be considered for implementation under 50.59 and which cannot. This could be more clearly stated.].

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 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 dependability, to determine whether the frequency of malfunctions occurring would be more than minimally increased (applicable to 50.59 Question 2)~~, or~~ . On the other hand, both dependability and design attributes are assessed to determine 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 (applicable to 50.59 Questions 5 and 6) [you cannot reach a CCF not credible conclusion with only a qualitative assessment of dependability attributes.]. Guidance within NEI 96-07 states that normally, the determination of a malfunction frequency increase is based 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 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 frequency of a malfunction must be "discernable and attributable" to the proposed activity in order to exceed the "more than minimal increase" standard (applicable to 50.59 Question 2). This concept was endorsed in RG 1.187, along with the endorsement of the balance of the NEI 96-07, Revision 1 document. On the other hand, for 50.59 Questions 5 and 6, any newly introduced malfunctions that are considered possible (i.e., credible) must be evaluated, regardless of their frequency.

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~~ defenses against CCF exist~~s~~ [there is no requirement for diversity], 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 [This statement contradicts previous statements that a D3 analysis is only needed for RPS and ESF systems.]. The clarified endorsement in this RIS identifies the need for documenting key design attributes and ~~quality management~~dependability measures that, when applied appropriately, could be considered as adequate to demonstrate a sufficient reduction in ~~uncertainty when performing qualitative assessments of~~the likelihood of occurrence of a potential CCF or a conclusion that a CCF is not credible, for such lower-safety significant (i.e., non-RPS and non-ESF ~~initiation~~ systems) 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~~ attributes and ~~quality management~~dependability measures that are applied to the proposed design using such standards and guidance should be described and evaluated within licensee documentation supporting any conclusions that a reduction in ~~uncertainty~~ CCF likelihood or a CCF not credible conclusion could be credited.

The NRC staff expectation regarding the documentation of ~~qualitative~~ dependability 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:

- 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 an I&C malfunction, there can be no postulated operational occurrences or accidents that are caused by 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~~as the result of a single failure ~~(which should already be addressed in the design)~~ [digital upgrades introduce new sources of CCF, including new single failures that can result in a CCF], the additional contribution of a new potential CCF to malfunction 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~~dependability and design attribute assessments is to be able to describe the licensee's basis (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 evaluating the impact of potential new CCFs that are of sufficient frequency (i.e., expected during the life of the plant) that need to be accounted for within the plant design basis, such as a CCF due to a single random hardware failure, design basis analysis methods and acceptance criteria should be used. When evaluating the impact of potential new CCFs that are of ~~negligible~~ significantly lower frequency (i.e., not expected during the life of the plant), such as a CCF due to a design defect in a system where robust dependability attributes have been assessed and documented, beyond design basis analysis methods (best estimate) and acceptance criteria may be used in evaluating whether the plant level effect is ~~bounding~~bounded. When a CCF is concluded to be not credible, or a credible CCF is concluded to result in SSC malfunctions that are already identified in current plant accident analyses (i.e., no new SSC malfunctions), no additional plant level end result analysis is needed.

[I am very happy to see the concepts of 'best estimate' and 'bounded' included in this document. However, unless you explain what bounded means, and the difference in 'bounded' for a design basis CCF vs. a beyond design basis CCF, this will not be evaluated consistently by industry; this poses a safety concern:

- It must be clear that bounded means a negligible reduction in the margins to critical safety function limits. Currently, bounded is not defined in NEI 96-07 or NEI 01-01.
- It must be clear that design basis CCFs must be bounded by current AOOs; alternately, beyond design basis CCFs can be bounded by current AOOs or PAs.
- It must be clear that mitigating actions for design basis CCFs can only credit safety systems; alternately mitigating actions for beyond design basis CCFs can credit non-safety systems of sufficient dependability or non-safety systems that are in continuous operation.]

Formatted: List Paragraph, Bulleted + Level: 1 + Aligned at: 0.25" + Indent at: 0.5"

Formatted: List Paragraph, Bulleted + Level: 1 + Aligned at: 0.25" + Indent at: 0.5"

To assist licensees in preparing acceptable ~~qualitative~~digital I&C change assessments supporting the rationale for responding to the 10 CFR 50.59 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, its position on the minimum content, rationale, and evaluation factors that should be addressed and evaluated within licensee-developed ~~qualitative~~digital I&C change assessments that serve as input to developing responses to the 10 CFR 50.59 evaluation criteria. Specifically, the clarified guidance within Attachment 1 describes the staff expectations for such ~~qualitative~~digital I&C change 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,~~ [layers of defense are for CCF mitigation, not failure likelihood reduction] and an evaluation of relevant operating experience were considered to contribute to such likelihood of failure, or to contribute to a CCF not credible conclusion.

For example, the clarified guidance in Attachment 1 identifies the need to provide adequate documentation in the modification package (that is then referenced in the ~~qualitative~~digital I&C change assessment) as to what specific design standards were followed in the development of the proposed digital &C modification to ensure that well-defined processes 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~~digital I&C change 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 design standards is considered to be adequate for the particular application, commensurate with the level of safety significance of the proposed modification, or its consequences of failure.

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 evaluated 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~~ controlled plant ~~equipment~~components (e.g., protective relays in switchgear). In BTP 7-19, Section 1.9 states that one design attribute is sufficient to eliminate consideration of ~~software based or software logic based~~ CCF due to a design defect: "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~~digital I&C change assessment, as described in Attachment 1 to this RIS, documenting the ~~technical and qualitative~~design attribute and dependability attribute basis (rationale) for concluding that ~~simple~~ digital devices have been adequately tested is acceptable. This ~~qualitative~~ dependability rationale may credit test results for all ~~reasonably testable~~ combinations of input states and internal states along with a documented technical justification that any states not practical to test are not expected to ever occur for the particular application. Therefore, "testability" is an acceptable basis for concluding that a CCF is not credible. When a CCF not credible conclusion is reached, no additional consideration of that CCF is required when responding to the 50.59 questions. [Add a similar paragraph for internal diversity, which is also an acceptable basis in BTP 7-19 for concluding that a CCF is not credible.]

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 [This makes no sense. If there is no change why would there be any screening; what would you screen?] 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 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~~digital I&C change assessments used for screening and evaluations, as described in Attachment 1 to this RIS. [Incorrect screening has been the source of most incorrect 50.59 evaluations. This paragraph is ambiguous. First it says a documented screening may not be required, then it says documented qualitative assessments are required for screening. This paragraph should be very clear that all digital upgrades require a documented screen, which includes (1) a qualitative dependability assessment of malfunction frequency, and (2) a qualitative dependability and deterministic design attribute assessment for the possibility of a new malfunction (i.e., CCF susceptibility).]

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~~of NEI 01-01, 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~~digital I&C change assessments used for screening and evaluations, as described in Attachment 1 to this 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 11 NRC staff concerns regarding inconsistent interpretation of provisions within

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

the guidance of NEI 01-01. On October 9, 2014, the NRC issued a meeting summary (ADAMS Accession No. ML14255A059) that identified a 12th concern.

Within this RIS, the staff considers the concerns regarding adequate means for addressing the evaluation criteria in 10 CFR 50.59 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:

Draft – ~~Qualitative~~Digital I&C change Assessment Framework

1 Introduction

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 digital replacements in a consistent manner. NEI 01-01 provides guidance in performing ~~qualitative~~digital I&C change assessments of the dependability of and risk associated with I&C systems. The NRC staff expects that such ~~qualitative~~digital I&C change 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.

2 Purpose

This enclosure provides clarification of the staff's previous endorsement of NEI guidance for performing and documenting ~~qualitative~~digital I&C change assessments developed in support of 10 CFR 50.59 evaluations of proposed digital modifications. Such ~~qualitative~~digital I&C change assessments are needed to document the technical bases for concluding whether there is reasonable assurance that any failures or failure modes due to the implementation of the proposed digital modification are consistent with the UFSAR analysis assumptions. 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 a license amendment request (LAR) will be required.

The ~~qualitative~~digital I&C change 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 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 a 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 50.90.

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~~[This incorrectly implies that the CCF is

automatically acceptable and that the LAR would be approved.]; a licensee amendment would be required. (via 10 CFR 50.90).

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

3 ~~Qualitative~~Digital I&C change Assessment

3.1 Scope

The ~~qualitative~~digital I&C change assessment process may be applied to any proposed digital I&C plant modifications to safety support systems [Without this you open the door to this process being applied to RT and ESF systems.] and non-safety systems. ~~However, a~~At this time, it is not intended for this RIS to apply to reactor protection or ~~essential~~ engineered 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 10 CFR 50.59 evaluation process for proposed changes to reactor protection and engineered ~~safeguards~~ safety feature ~~initiation~~ systems, it will be found that a license amendment request will be necessary to make the change [This highlighted sentence should be deleted, because there is nothing in the digital I&C change assessment process that you have defined that would change the result for RT and ESF systems; the result could most certainly be that an LAR is not required. It is only this RIS that would limit the application to exclude RPS and ESF functions.].

Formatted: Highlight

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. [This paragraph is going to confuse many people. I have been in this industry for 42 years and have never seen the term 'qualitative assessment' used for the assessment of 'design attributes'. The term 'qualitative assessment' is historically limited to dependability issues (e.g., design process, complexity) which require subjective engineering judgement. By your definition, a failure modes and effects analysis (FMEA) would be a digital I&C change assessment; I'm sure the writers of IEEE-379 would strongly disagree. Similarly, qualitative assessment is not found in IEEE-384, IEEE-323 and IEEE-603, because these all define deterministic design attributes. An assessment of design attributes is historically referred to as a deterministic assessment, as in NEI 00-01. The important point here is that the assessment needed for this CCF evaluation does not require quantitative numbers; that does not mean that the assessment is solely qualitative. The needed assessment is a combination of dependability attributes (e.g., design process, complexity) which are assessed qualitatively, and

design attributes (e.g., independence, segmentation, watchdog timers) which are assessed deterministically.]

3.3 ~~Qualitative~~Digital I&C Change Argument Cornerstones

This ~~Qualitative~~Digital I&C Change Assessment clarification highlights four general categories of proposed design-related characteristics, each of which need to be evaluated to formulate effective ~~qualitative~~digital I&C change arguments deemed sufficient to address the questions posed in the "Purpose" section above. The staff finds that 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 evaluation questions. These areas should be evaluated 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. Evidence of design attributes supporting arguments for the high reliability and dependability of the proposed modification should be described.

- Dependability Attributes include qQuality 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. Alternately, evidence that the proposed system or component modification employs equipment with significant operating history in nuclear power plant applications or non-nuclear applications with comparable performance requirements, and the suppliers of such equipment incorporate quality processes such as continual process improvement, incorporation of lessons learned, etc.

- ~~Defense in Depth: Evidence that the proposed design incorporates both internal and external layers of defense against potential failures of the modified I&C system or component 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 new AOOs or PAs that have not been previously analyzed.~~ [This paragraph is going to confuse people because defense-in-depth historically refers to the echelons of defense described in BTP 7-19 (i.e., control, protection, operator actions) and the reactivity control diversity required by GDC 26. A watchdog timer or interlock built into a system to force a specific failure mode (i.e., a limiting measure), is a design attribute of the system, not defense-in-depth.]

- ~~Operating Experience: 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~~

Formatted: No underline

~~improvement, incorporation of lessons learned, etc.~~ [Operating experience is just another way of demonstrating the "quality processes" which you define above.]

[It would be much easier for people to understand this section, if you limit your discussion to dependability attributes (qualitative assessment) and design attributes (deterministic assessment).]

Formatted: Font: (Default) Arial, Underline

Formatted: Underline

Formatted: Normal, Indent: Left: 0.25", No bullets or numbering

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

Table 1 - ~~Qualitative~~Digital I&C change ~~Argument~~CCF Assessment Topical Areas	
Topical Area	Description
Design Attributes	• Design Criteria – For example: Diversity ~~(if applicable)~~[this is true of all of these attributes], 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 • Configuration and functional differences to achieve ~~Non~~non-concurrent triggers • Sufficiently Simple (i.e. enabling 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.~~ [This is a risk assessment, as is done in the PRA; this is not a design attribute.] • Failure state always known to be safe • Features to ensure equipment can be qualified (e.g., structural features for seismic durability, noise filters for EMI durability) • 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.) that limit or prevent a CCF
~~Quality Design Processes~~Dependability Attributes	• Compliance with industry codes and standards - It is the expectation that for non-NRC endorsed codes and standards, the licensee must provide an explanation for why use of the particular non-endorsed standard(s) is acceptable. • Use of Appendix B vendors, or if not Appendix B, which generally accepted industrial quality program applies • Environmental qualification (e.g. EMI/RFI, Seismic) • Development Process rigor • 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.

~~Defense-In-Depth~~	~~• Coping measures~~ ~~• Availability of operator intervention capabilities independent of the potential CCF, administrative controls, and sufficient time to respond~~ [The two items above do not prevent, limit or reduce the likelihood of a CCF. Therefore, they cannot be credited in the CCF susceptibility analysis. They can be credited only in the CCF malfunction result analysis. By including these in this list you are confusing the two issues. Reducing the likelihood of a CCF and limiting the effects of a CCF are based on attributes of the target system. Methods to coping with a credible CCF are external to the target system.] • ~~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.)~~ [These are design attributes.]
~~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.~~

3.3.1 Design Attributes versus ~~Quality Process~~Dependability Attributes

Both "Design Attributes" and "~~Quality Process~~Dependability Attributes" are needed because to some degree 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. [It is ridiculous to use a mechanical example in an I&C document. Dependability attributes reduce the likelihood of a failure. Design attributes reduce the likelihood that the failure will cause a CCF.]

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 software logic based~~ CCF due to a design defect: Diversity or Testability. However, if CCF is considered in a larger context (i.e., ~~software based or software logic based~~ CCFs caused by a design defect are not the only types of CCFs), then there are many regulatory requirements to address potential CCFs, and thereby eliminate them

from further consideration. As a result, any ~~relaxations~~ changes [relaxation is highly ambiguous and open to interpretation. "changes" is consistent with the next sentence] in how these requirements are met, or any changes that introduce new potential sources of CCF (e.g., new shared resources or new digital designs), should screen in (i.e., require a full 50.59 evaluation). Changes in how requirements are met and new potential sources of CCF need to be 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 regulatory criteria. Historically, t~~T~~hese SSCs ~~may have been~~are implemented in a manner (i.e., relatively independently) such that only an 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 or HSI) each other, then the new malfunction and/or accident must be evaluated under 50.59. ~~NRC approved qualitative and/or quantitative methods~~Dependability attributes and design attributes ~~can be~~are used to ~~evaluate attributes of the design to~~ determine whether a license amendment ~~may be~~is 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 10 CFR 50.90~~screen in for a 50.59 evaluation. [It is not appropriate for the Staff to shortcut the 50.59 process in this RIS for these changes. If you exclude RPS/ESF (from sensor to controlled component, including any functions that can block the safety function), that is enough.]

- Combination of Functions: The combination of functions (that (i) can cause a plant transient, (ii) are credited for mitigating plant transients either directly or as an auxiliary support function, or (iii) are of different layers of defense) should ~~be evaluated under~~screen in for a 50.59 evaluation. ~~If the evaluation determines that: (A) a new type of accident, (B) a malfunction with a new result, or (C) an unbounded malfunction or accident now exists, then a LAR is required.~~ [It is not appropriate for the Staff to shortcut the 50.59 process for these changes.]

- 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 radioactive material. 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, 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 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 question 1 &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.”

Formatted: Indent: Left: 0.5"

[I agree a change that reduces defense in depth warrants an LAR. But bullets 1 and 2 above do not warrant an LAR.

However, if should be clear that a reduction in defense in depth can only occur due to a CCF that adversely affects multiple echelons of defense identified in BTP 7-19, or adversely affects the reactivity control diversity required by GDC 26. If there is no CCF, or no CCF that affects these functions, there is no reduction in defense in depth.]

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 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 must be stipulated and documented as being achieved (per GDC 1 - Quality Standards and Records) [Note that in GDC 1 there is a clear distinction between design attributes (which are deterministic) and the methods used to ensure those attributes are implemented correctly (which is qualitative).]:

(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 [there is only one sentence above] 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.

(2) "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."

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."

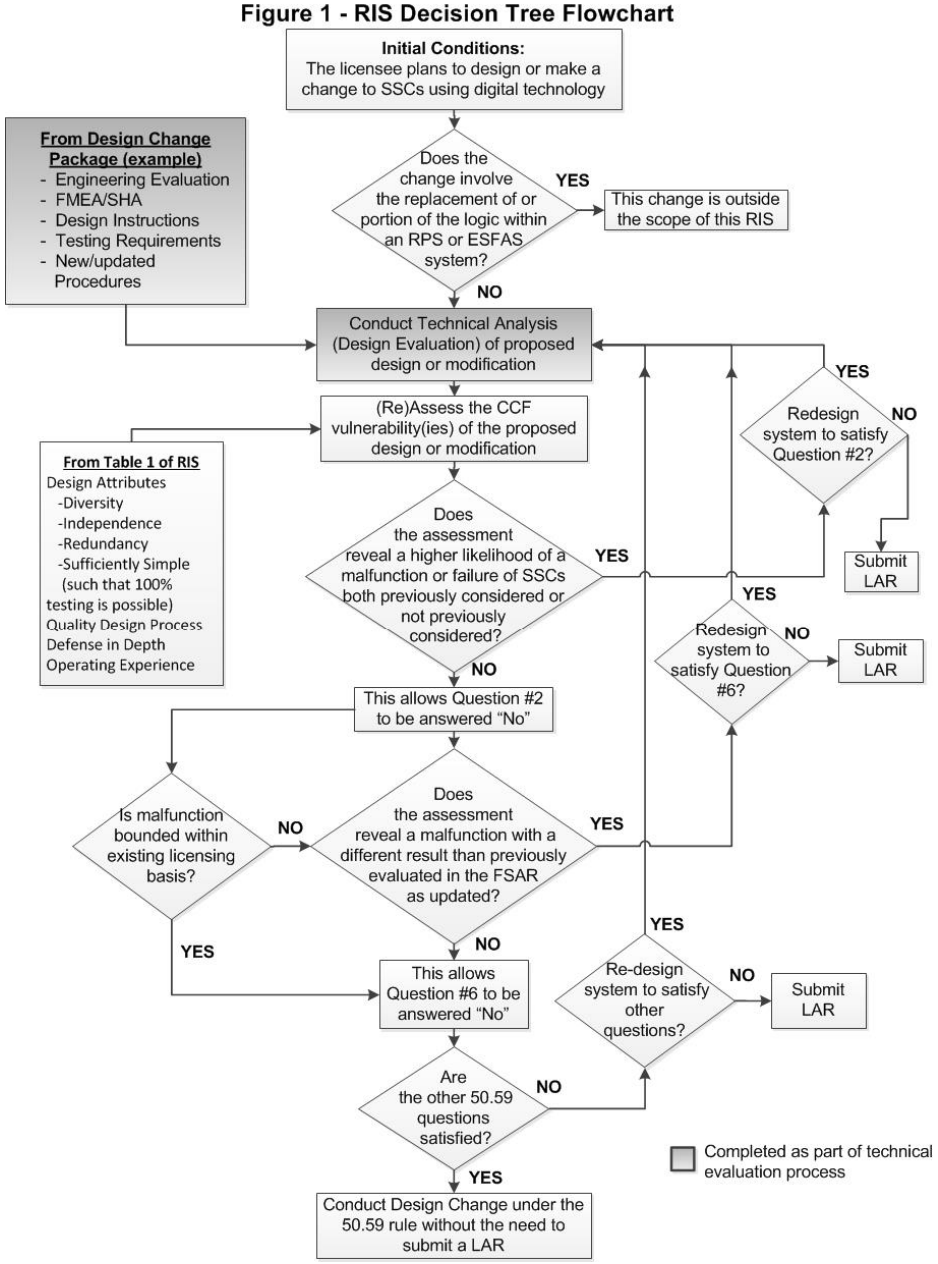
The sentence requires documentation for important to safety equipment that is not part of an Appendix B QA program.

[Does this RIS really need a lesson on GDC 1? I don't think so.]

3.3.5 Decision Process

Figure 1 of this ~~qualitative~~digital I&C change 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~~digital I&C change assessment guidance.

Figure 1 - RIS Decision Tree Flowchart



[see separate PDF file for comments on the figure above.]

4 ~~Qualitative~~Digital I&C Change Assessment Documentation

The ~~qualitative~~digital I&C change 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 50.59 evaluation questions. It's the staff's expectation that ALL of these categories be addressed to the degree possible. **See Table 2**. This table provides the 'process flow' that should be followed in terms of the structure of the ~~qualitative~~digital I&C change assessment presentation as well as specific steps that should be addressed in the process.

4.1 Responsibilities of License Holders

It is critical that the licensee document in the design modification package the design codes and standards that were used in the development of the proposed digital I&C design modification. The ~~qualitative~~digital I&C change assessment will reference the design standards used, and provide a rationale as to why 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 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 design standard employed is considered adequate for the proposed design modification, commensurate with the level of safety significance.

4.2 Safety Significance of SSCs and Documentation of Evidence

As stated previously, an important consideration for documentation of evidence to address 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 not limited to the following:

- Is the SSC(s) to be modified ~~an~~ a direct or indirect event initiator?
- Is the SSC(s) to be modified part of an accident mitigation system, or a support system?
- ~~Is the SSC(s) to be modified important to maintaining barrier integrity?~~ [this is covered by the second bullet above.]

[As written, this implies that there would be a difference in rigor between the bullets. But that should not be accepted, because a CCF that results in a new unanalyzed event is as safety significant as a CCF that results in failure of a mitigation system. It should be clear that each bullet stands on its own.]

Formatted: Font: (Default) Arial

Formatted: Normal, Indent: Left: 0.25", No bullets or numbering

Formatted: Normal, No bullets or numbering

~~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:~~

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

[Now you are trying to prioritize critical safety functions. I have never seen this before. There is no technical basis for this. All critical safety functions are equally important.]

It is the responsibility of the 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 the 50.59 evaluation.

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

Table 2 - ~~Qualitative~~Digital I&C Change 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	[For 50.59 Q2 you must first assess failure frequency. The failure mode is irrelevant.] 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? [this is a statement, not a question] • Its postulated CCF likelihood is significantly lower than single failures considered in the UFSAR or comparable to CCFs that are not considered in the safety analyses (e.g. design flaws, maintenance errors)? [this is a statement, not a question] 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~~digital I&C change assessment will not determine the absolute likelihood of failure.
Step 5 – Documentation of Evidence	Evidence should support each of the assertions (e.g. evidence of the ~~4~~ two ~~qualitative~~digital I&C change assessment arguments, design attributes and dependability attributes) including: Dependability attributes: (1) codes and standards applied, qualification for the environment (e.g., seismic, EMI/RFI, ambient temperature, heat contribution, etc.), other testing as applicable. (2) 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~~ [this is a design attribute within the target change]~~, manual back-up capability~~ [this is a coping attribute outside the target change]~~, etc.)~~, and/or (3) Operating History (e.g., platform used in numerous applications worldwide, etc. with minimal failure history, etc.). Design attributes: independence/segmentation of functions, redundancy of shared resources, watchdog timers, internal diversity, minimal inputs and internal states to achieve testability, etc. The level of evidence provided should be commensurate to the safety significance of the SSC(s) to be modified.

Formatted: Underline

Formatted: Underline

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

~~Step 6 - Rationale~~	[this should be part of Step 5] State why ~~the~~ each 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~~digital I&C change 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~~digital I&C change assessment to respond to each of the 50.59 evaluation questions.

[This table above is suitable for the assessment of malfunction frequency and CCF likelihood. It is not sufficient to evaluate the CCF malfunction results at the component/system level or at the plant level. For the CCF malfunction results at the plant level the table must be significantly expanded to address bounded criteria and analysis methods for both design basis and beyond design basis CCFs.]