

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

Month XX, 2018

**DRAFT NRC REGULATORY ISSUE SUMMARY 2002-22, SUPPLEMENT 1
CLARIFICATION ON ENDORSEMENT OF NUCLEAR ENERGY INSTITUTE GUIDANCE IN
DESIGNING DIGITAL UPGRADES IN INSTRUMENTATION AND CONTROL SYSTEMS**

ADDRESSEES

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

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

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

INTENT

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

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

proposed digital I&C modification has a sufficiently low¹ likelihood of failure. This conclusion, and the reasons for it, should be documented, per 10 CFR 50.59(d)(1), as part of the evaluations of proposed digital I&C modifications against some of the criteria in 10 CFR 50.59, "Changes, tests and experiments."

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

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

BACKGROUND INFORMATION

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

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

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

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

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

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

Applicability to Non-Power Reactor Licensees

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

SUMMARY OF ISSUE

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

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

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

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

BACKFITTING AND ISSUE FINALITY DISCUSSION

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

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

FEDERAL REGISTER NOTIFICATION

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

CONGRESSIONAL REVIEW ACT

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

PAPERWORK REDUCTION ACT STATEMENT

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

Public Protection Notification

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

CONTACT

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

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

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

Technical Contacts: David Rahn, NRR
301-415-1315

e-mail: David.Rahn@nrc.gov

Wendell Morton, NRR
301-415-1658

e-mail: Wendell.Morton@nrc.gov

Norbert Carte, NRR
301-415-5890

e-mail: Norbert.Carte@nrc.gov

David Beaulieu, NRR
301-415-3243

e-mail: David.Beaulieu@nrc.gov

Duane Hardesty, NRR
301-415-3724

email: Duane.Hardesty@nrc.gov (Specifically for non-power reactors)

Project Manager Contact: Tekia Govan, NRR
301-415-6197

e-mail: Tekia.Govan@nrc.gov

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

Attachment: Qualitative Assessment and Engineering Evaluation Framework

Qualitative Assessment and Engineering Evaluation Framework

1. Purpose

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

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

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

If a "qualitative assessment" determines that a potential failure (e.g., software common cause failure (CCF) has a sufficiently low likelihood, then the effects of the failure do not need to be considered in the 10 CFR 50.59 evaluation. Thus, the "qualitative assessment" provides a means of addressing software CCF. In some cases, the effects of a software CCF may not create a different result than any previously evaluated in the updated final safety analysis report (UFSAR).

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

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

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

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

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

2.1 Likelihood

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

Qualitative Assessment

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

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

Qualitative Assessment Outcome

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

credible or not is whether it is “as likely as” (i.e., not “much lower than”) malfunctions already assumed in the UFSAR.

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

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

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

Criteria

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

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

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

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

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

Does the activity result in more than a minimal increase in the likelihood of occurrence of a malfunction of a structure, system, or component (SSC) important to safety³ previously evaluated in the UFSAR?

“Sufficiently low” threshold – The likelihood of occurrence of a malfunction of an SSC important to safety is directly related to the likelihood of failure of equipment that causes a failure of SSCs to perform their intended design functions⁴ (e.g., an increase in the

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

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

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

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

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

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

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

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

“Sufficiently low” threshold – NEI 96-07, Section 4.3.6, states, “...malfunctions with a different result are limited to those that are as likely to happen as those in the UFSAR.” A malfunction of an SSC important to safety is an equipment failure that causes the failure of SSCs to perform their intended design functions. If the outcome of the qualitative assessment of the proposed change is that the likelihood of failure associated with the proposed activity is “sufficiently low,” then there are no failures introduced by the activity that are as likely to happen as those in the UFSAR. Therefore, the activity does not create a possibility for a malfunction of an SSC important to safety with a different result than any previously evaluated in the UFSAR. If the qualitative assessment determines that a potential failure (e.g., software CCF) does not have a sufficiently low likelihood, then the effects of this failure need to be considered in the 10 CFR 50.59 evaluation using methods consistent with the plant’s UFSAR.

3. Qualitative Assessments

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

1. Digital I&C modifications that:

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

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

- b) Do not create a CCF vulnerability due to new shared resources (such as power supplies, controllers, and human-machine interfaces) with other design functions that are (i) explicitly or implicitly described in the UFSAR as functioning independently from other plant design functions, or (ii) modeled in the current design basis to be functioning independently from other plant design functions.
- c) Do not affect reactor trip or engineered safety feature initiation/control logic or emergency power bus load sequencers.

2. Digital I&C modifications that maintain the level of diversity, separation, and independence of design functions described in the UFSAR. A change that reduces redundancy, diversity, separation or independence of USFAR-described design functions is considered a more than minimal increase in the likelihood of malfunction.
3. Digital I&C modifications that are sufficiently simple (as demonstrated through 100 percent testing or a combination of testing and input/output state analysis); or demonstrate adequate internal diversity.

3.1 Qualitative Assessment Categories

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

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

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

3.1.1 Design attributes

NEI 01-01 Section 5.3.1 states:

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

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

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

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

3.1.2 Quality of the Design Process

Section 5.3.3 of NEI 01-01 states:

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

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

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

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

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

3.1.3 Operating Experience

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

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

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

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

Table 1—Qualitative Assessment Category Examples

Table 1—Qualitative Assessment Category Examples	
<u>Categories</u>	<u>Examples for Each Category</u>
Design Attributes	<ul style="list-style-type: none"> • Design criteria—Diversity (if applicable), Independence, and Redundancy. • Inherent design features for software, hardware or architectural/network— Watchdog timers that operate independent of software, isolation devices, segmentation of distributed networks, self-testing, and self-diagnostic features. • Basis for identifying that possible triggers are non-concurrent. • Sufficiently simple (i.e., enabling 100 percent testing or comprehensive testing in combination with analysis of likelihood of occurrence of input/output states not tested). • Failure state always known to be safe, or at least the same state as allowed by the previously installed equipment safety analysis.
Quality of the Design Process	<ul style="list-style-type: none"> • Justification for use of industry consensus standards—for codes and standards not endorsed by the NRC. • Justification for use of other standards. • Use of Appendix B vendors. If not an Appendix B vendor, the analysis can state which generally accepted industrial quality program was applied. • Use of Commercial Grade Dedication processes per guidance of EPRI TR-106439, Annex D of IEEE 7-4.3.2, and examples within EPRI TR-107330. • Demonstrated capability (e.g., through qualification testing) to withstand environmental conditions within which the SSC is credited to perform its design function (e.g., EMI/RFI, Seismic). • Development process rigor (adherence to generally-accepted commercial or nuclear standards.) • Demonstrated dependability of custom software code for application software through extensive evaluation or testing.
Operating Experience	<ul style="list-style-type: none"> • Wide range of operating experience in similar applications, operating environments, duty cycles, loading, comparable configurations, etc., to that of the proposed modification. • History of lessons learned from field experience addressed in the design. • Relevant operating experience: Architecture of the referenced equipment and software (operating system and application) along with the design conditions and modes of operation of the equipment should be substantially similar to those of the system being proposed as a digital I&C modification. High volume production usage in different applications—Note that for software, the concern is centered on lower volume, custom, or user-configurable software applications. High volume, high quality commercial products with relevant operating experience used in other applications have the potential to avoid design errors. • Experience working with software development tools used to create configuration files.

3.2 Qualitative Assessment Documentation

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

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

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

4. Engineering Evaluations

4.1 Overview

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

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

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

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

4.2 Selected Design Considerations

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

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

4.2.1 Digital Communications

Careful consideration of digital communications is needed to preclude adverse effects on SSC independence. DI&C-ISG-04, Revision 1, "Highly-Integrated Control Rooms - Communications Issues" (Agencywide Documents Access and Management System Accession Number ML083310185) provides guidance for NRC staff reviewing digital communications. This ISG describes considerations for the design of communications between redundant SSCs, echelons of defense-in-depth⁵ or SSCs with different safety classifications. The principles of this ISG or other technically justifiable considerations, may be used to assess non-safety related SSCs.

4.2.2 Combining Design Functions

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

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

4.3 Failure Analyses

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

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

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

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

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

4.4 Defense-in-Depth Analyses

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

4.5 Dependability Evaluation

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

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

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

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

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

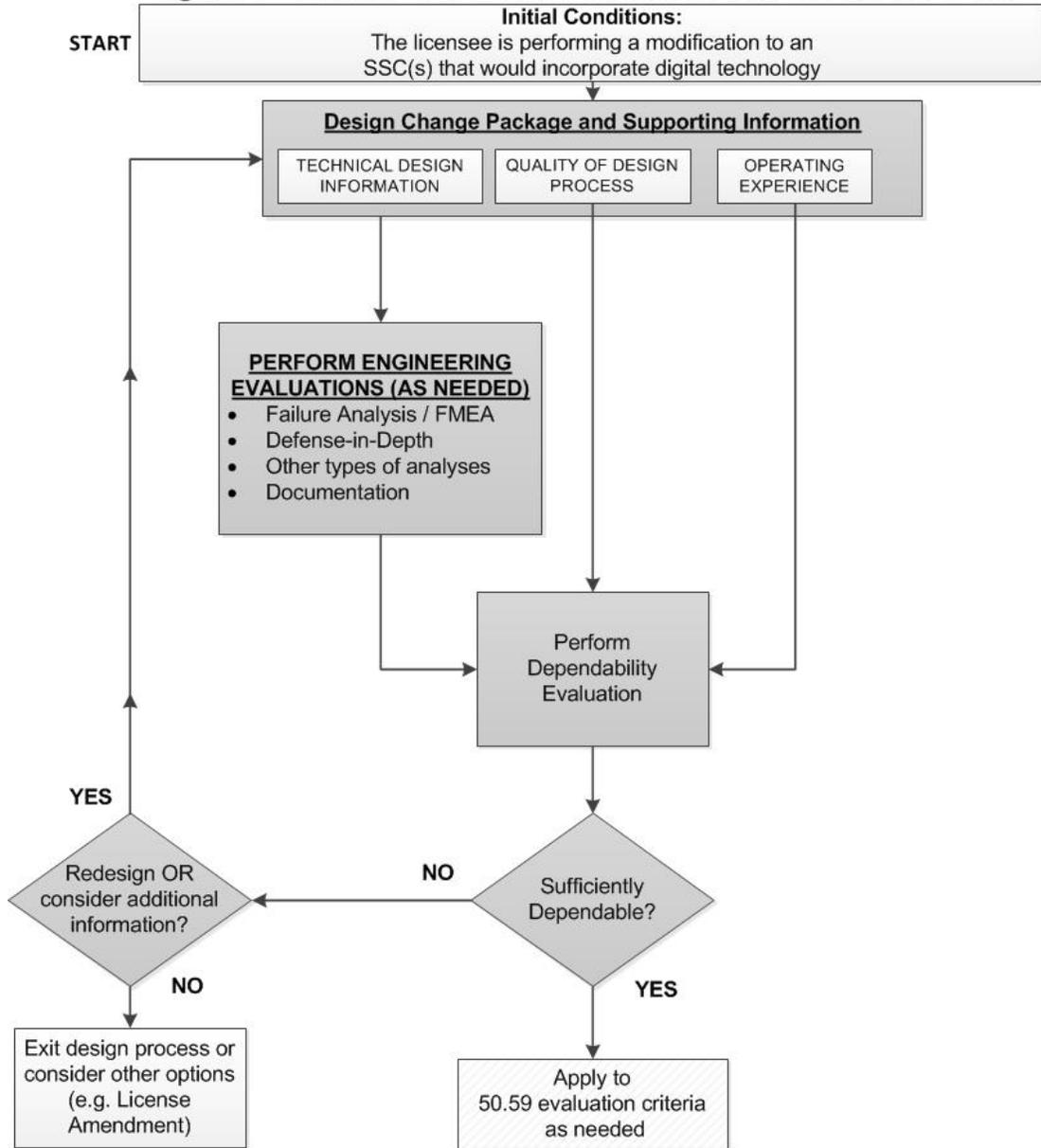
Figure 1 of this attachment provides a simplified illustration of the engineering evaluations process described in Section 4 of this attachment.

4.6 Engineering Documentation

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

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

Figure 1 – EXAMPLE ENGINEERING EVALUATION PROCESS



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

Completed as part of technical design process

Completed as part of the 50.59 evaluation

Table 2—Example - Engineering Evaluation Documentation Outline to support a Qualitative Assessment	
<u>Topical Area</u>	<u>Description</u>
Step 1- Identification	<p>Describe the full extent of the SSCs to be modified—boundaries of the design change, interconnections with other SSCs, and potential commonality to vulnerabilities with existing equipment.</p> <ul style="list-style-type: none"> • What are all of the UFSAR-described design functions of the upgraded/modified components within the context of the plant system, subsystem, etc.? • What design function(s) provided by the previously installed equipment are affected and how will those design functions be accomplished by the modified design? Also describe any new design functions that were not part of the original design. • What assumptions and conditions are expected for each associated design function? For example, the evaluation should consider both active and inactive states, as well as transitions from one mode of operation to another.
Step 2—Identify potential failure modes and undesirable behavior	<p>Consider the possibility that the proposed modification may have introduced potential failures.</p> <ul style="list-style-type: none"> • Are there potential failure modes or undesirable behaviors as a result of the modification? A key consideration is that undesirable behaviors may not necessarily constitute an SSC failure, but a misoperation. (e.g., spurious actuation) • Are failures including, but not limited to, hardware, software, combining of functions, shared resources, or common hardware/software considered? • Are there interconnections or interdependencies among the modified SSC and other SSCs? • Are there sources of CCF being introduced that are also subject to common triggering mechanisms with those of other SSCs not being modified? • Are potential failure modes introduced by software tools or programmable logic devices?
Step 3—Assess the effects of identified failures	<ul style="list-style-type: none"> • Could the possible failure mode or undesired behavior lead to a plant trip or transient? • Can the possible failure mode or undesired behavior affect the ability of other SSCs to perform their design function? • Could the possible failure mode of the SSC, concurrent with a similar failure of another SSC not being modified but sharing a common failure and triggering mechanism affect the ability of the SSC or other SSCs to perform their design functions? • What are the results of the postulated new failure(s) of the modified SSC(s) compared to previous evaluation results described in the UFSAR?
Step 4—Identify appropriate	<p>What actions are being taken (or were taken) to address significant identified failures?</p> <ul style="list-style-type: none"> • Are further actions warranted?

Table 2—Example - Engineering Evaluation Documentation Outline to support a Qualitative Assessment	
<u>Topical Area</u>	<u>Description</u>
resolutions for each identified failures	<ul style="list-style-type: none"> • Is re-design warranted to add additional design features or attributes? • Is the occurrence of failure self-revealing or are there means to announce the failure or misbehavior to the operator?
Step 5— Documentation	<ul style="list-style-type: none"> • Describe the resolutions identified in Step 4 of this table that address the identified failures. • Describe the conformance to regulatory requirements, plant's UFSAR, regulatory guidance, and industry consensus standards (e.g., seismic, EMI/RFI, ambient temperature, heat contribution). • Describe the quality of the design processes used within the software life cycle development (e.g., verification and validation process, traceability matrix, quality assurance documentation, unit test and system test results). • Describe relevant operating history (e.g., platform used in numerous applications worldwide with minimal failure history). • Describe the design features/attributes that support the dependability conclusion (e.g., internal design features within the digital I&C architectures such as self-diagnostic and self-testing features or physical restrictions external to the digital I&C portions of the modified SSC), defense-in-depth (e.g., internal diversity, redundancy, segmentation of distributed networks, or alternate means to accomplish the design function). • Summarize the results of the engineering evaluation including the dependability determination.

**DRAFT NRC REGULATORY ISSUE SUMMARY 2002-22, SUPPLEMENT 1, CLARIFICATION
ON ENDORSEMENT OF NUCLEAR ENERGY INSTITUTE GUIDANCE IN DESIGNING
DIGITAL UPGRADES IN INSTRUMENTATION AND CONTROL SYSTEMS DATE: Month
XX, 2018**

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