The following document is a preliminary draft being made publically available to support a Category 3 public meeting on May 23, 2018. NRC staff review of this draft document has not been completed.

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

UNITED STATES
NUCLEAR REGULATORY COMMISSION
OFFICE OF NUCLEAR REACTOR REGULATION
OFFICE OF NEW REACTORS
WASHINGTON, DC 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 of power reactor operating licenses under Title 10 of the *Code of Federal Regulations* (10 CFR) Part 50, "Domestic Licensing of Production and Utilization Facilities."

All holders of combined licenses under 10 CFR Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants."

All holders of operating licenses under 10 CFR Part 50, for nonpower reactors for the production of medical radioisotopes, such as molybdenum-99, except for 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, "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,'" dated November 25, 2002 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML023160044). RIS 2002-22 endorses Nuclear Energy Institute (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," issued March 2002 (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 referred to as "digital I&C") in a consistent and comprehensive manner.

The RIS supplement clarifies 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 NEI 01-01, Sections 4 and 5 and Appendices A and B. 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

ML18116A268

sufficiently low[1] likelihood of failure. This conclusion and the reasons for it should be documented, as required by 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."

Consistent with RIS 2002-22, this RIS supplement is intended to address digital modifications to safety-related systems or components but may also be applied to modifications of non-safety related systems or components at the discretion of the licensee. This RIS supplement is not directed toward digital I&C replacements of the reactor protection system, the engineered safety features actuation system, or modification/replacement of the internal logic portions of these systems (e.g., voting logic, bistable inputs, and signal conditioning/processing) because application of the guidance in this RIS supplement to such changes would likely involve additional considerations. This RIS supplement provides guidance for addressing CCF in 10 CFR 50.59 evaluations. Other NRC guidance documents address potential CCFs of digital I&C equipment.

This RIS supplement does not require any action or written response on the part of an addressee.

BACKGROUND INFORMATION

By letter dated March 15, 2002, NEI submitted Electric Power Research Institute (EPRI) TR-102348, Revision 1 (NEI 01-01), for the NRC staff's review. NEI 01-01 replaced the original version of EPRI TR-102348, issued 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). On November 25, 2002, the NRC staff issued RIS 2002-22 to notify addressees that it had reviewed NEI 01-01 and was endorsing the report for use as guidance in designing and implementing digital upgrades to nuclear power plant I&C systems.

Following the NRC staff's 2002 endorsement of NEI 01-01, holders of 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," issued November 2000 (ADAMS Accession No. ML003759710), which endorses NEI 96-07, "Guidelines for 10 CFR 50.59 Implementation," Revision 1, issued November 2000 (ADAMS Accession No. ML003771157).

NRC inspections of documentation for digital I&C plant modifications that some licensees prepared using the guidance in NEI 01-01 identified inconsistencies in the performance and documentation of licensee engineering evaluations. In addition, NRC inspections identified documentation issues with the written evaluations of the 10 CFR 50.59(c)(2) criteria. The term "engineering evaluations" refers to evaluations performed in designing digital I&C modifications *other* than the 10 CFR 50.59 evaluations (e.g., 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.

[1] On page 4-20 of NEI 01-01, NEI defines "sufficiently low" to mean much lower than the likelihood of failures that are considered in the updated final safety analysis report (UFSAR) (e.g., single failures) and comparable to other CCFs that are not considered in the UFSAR (e.g., design flaws, maintenance errors, calibration errors).

In response to Staff Requirements Memorandum (SRM)-SECY-16-0070 "Staff Requirements—SECY-16-0070—Integrated Strategy To Modernize the Nuclear Regulatory Commission's Digital Instrumentation and Control Regulatory Infrastructure," dated October 25, 2016 (ADAMS Accession No. ML16299A157), the NRC staff has engaged the public, 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 the I&C regulatory infrastructure. The integrated action plan described the issuance of the guidance in this RIS supplement as a near-term action to provide specific guidance for documenting qualitative assessments that support a conclusion that a proposed digital I&C modification will exhibit a sufficiently low likelihood of failure.

Applicability to Nonpower 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 the original RIS 2002-22) primarily focus on power reactors. Nonetheless, NPUF licensees may also use the guidance in RIS 2002-22 and apply the guidance in this RIS supplement to develop written evaluations that address 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 NEI 01-01, Section 4, Section 5, and Appendix A. However, certain aspects of the guidance that discuss the relationship of other regulatory requirements in 10 CFR 50.59 may not fully apply to NPUFs (e.g., 10 CFR Part 50, Appendix A, "General Design Criteria for Nuclear Power Plants," and Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants," do not apply to NPUFs).

SUMMARY OF ISSUE

In general, implementation of digital I&C technology can provide dependability and safety benefits. Notably, digital technology can be designed to provide continuous diagnostic information to plant operators on the integrity of its internal systems operation and its availability. However, implementation of digital I&C technology may introduce potential operational hazards such as software CCF or failures introduced as result of interconnectivity. Some operational hazards, such as software CCF, may be addressed through a qualitative assessment.

A qualitative assessment can be used to support a conclusion that a proposed digital I&C modification will not result in 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 updated final safety analysis report (10 CFR 50.59(c)(2)(v) and (vi)). These conclusions can be satisfied if a proposed digital I&C modification has a sufficiently low likelihood of failure.

For digital I&C modifications, an adequate basis for a determination that a proposed change involves a sufficiently low likelihood of failure may be derived from a qualitative assessment of factors such as design attributes, the quality of the design processes used, and an evaluation of relevant operating experience of the integrated software and hardware used (i.e., product

maturity and inservice experience). The licensee may use a qualitative assessment to document the factors and rationale for concluding that an adequate basis exists for determining that a digital I&C modification will exhibit a sufficiently low likelihood of failure. In doing so, the 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 including approaches for addressing interconnectivity operational hazards.

BACKFITTING AND ISSUE FINALITY DISCUSSION

This RIS supplement clarifies but does not supersede RIS 2002-22 and includes additional guidance on how to perform and document qualitative assessments and supporting engineering evaluations 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 published a notice of opportunity for public comment on this RIS in Volume 83 of the *Federal Register*, page 11154, on March 14, 2018 (83 FR 11154). The NRC received comments from seven commenters. The NRC considered all comments, some of which resulted in changes to the RIS, and discussed the evaluation of these comments and the resulting changes to the RIS in a memorandum that is publicly available in ADAMS under Accession No. ML18115A298.

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 (OMB) 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.). OMB approved this information collection 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 contacts or the 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
e-mail: Duane.Hardesty@nrc.gov (specifically for nonpower 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 Failure Analysis

QUALITATIVE ASSESSMENT AND FAILURE ANALYSIS

1. Purpose

Regulatory Issue Summary (RIS) 2002-22, "NRC Regulatory Issue Summary 2002-022: 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,'" dated November 25, 2002 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML023160044), endorses Nuclear Energy Institute (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," issued March 2002 (ADAMS Accession No. ML020860169). NEI 01-01 provides guidance on implementing and licensing digital upgrades and provides guidance on performing qualitative assessments of the dependability of digital instrumentation and control (I&C) systems.

NEI 96-07, "Guidelines for 10 CFR 50.59 Implementation," Revision 1, issued November 2000 (ADAMS Accession No. ML003771157), acknowledges that qualitative assessments may be used to address some of the criteria in Title 10 of the *Code of Federal Regulations* (10 CFR) 50.59, "Changes, tests, and experiments." This attachment provides supplemental clarifying guidance on one acceptable approach for performing qualitative assessments of digital I&C modifications. 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. Although a qualitative assessment can be used to support a 10 CFR 50.59 evaluation, this RIS supplement does not provide guidance for screening nor does it presume that all digital modifications "screen in."

NEI 01-01 uses the terms "qualitative assessment" and "dependability evaluations" interchangeably. Within this RIS supplement attachment the terms "qualitative assessment" and "sufficiently low"[1] are used in conjunction with the performance of 10 CFR 50.59 evaluations. The term "dependability evaluation" is used in the context of engineering evaluations. Engineering evaluations are not part of a 10 CFR 50.59 evaluation but may provide technical supporting information for a 10 CFR 50.59 evaluation. Engineering evaluations are performed in accordance with the licensee's U.S. Nuclear Regulatory Commission (NRC)-approved quality assurance program in developing digital I&C modifications.

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

[1] On page 4-20 of NEI 01-01, NEI defines "sufficiently low" to mean much lower than the likelihood of failures that are considered in the updated final safety analysis report (UFSAR) (e.g., single failures) and comparable to other common-cause failures (CCFs) that are not considered in the UFSAR (e.g., design flaws, maintenance errors, calibration errors).

2. Regulatory Clarification—Application of Qualitative Assessments to 10 CFR 50.59

When a licensee decides to undertake an activity that changes its facility as described in the UFSAR, the licensee 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.

These evaluations must address all elements of proposed changes. Some elements of a change may have positive effects on the likelihood of structure, system, and component (SSC) failures, whereas other elements of a change may have negative effects. As derived from the guidance in NEI 96-07, positive and negative elements can be considered together if they are interdependent. Elements that are not interdependent must be evaluated separately.

2.1 Qualitative Assessment

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. The 10 CFR 50.59 written evaluation uses this conclusion to determine whether prior NRC approval is required.

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 such as system design attributes, the quality of the design processes employed, and the operating experience with the integrated software and hardware used (i.e., product maturity and inservice 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, coupled with an analysis demonstrating that untested states that are not tested, if any, are not possible for the proposed application, may provide additional assurance of a sufficiently low likelihood of failure that helps compensate for a lack of operating experience.

<u>Sufficiently Low Outcome</u>

One approach for a qualitative assessment employs the concept of a sufficiently low likelihood of failures. The use of this concept results in two possible outcomes of the sufficiently low determination: (1) failure likelihood is “sufficiently low” and (2) failure likelihood is not “sufficiently low.” NEI 01-01, Section 4.3.6, states that “sufficiently low” means much lower than the likelihood of failures that are considered in the UFSAR (e.g., single failures) and comparable to other CCFs that are not considered in the UFSAR (e.g., design flaws, maintenance error, calibration errors). This “sufficiently low” threshold is not interchangeable with that used for distinguishing between events that are “credible” or “not credible.” The threshold for

determining whether an event is credible is whether it is "as likely as" (i.e., not "much lower than") the malfunctions already assumed in the UFSAR.

If a "qualitative assessment" determines that a potential failure (e.g., software CCF) has a sufficiently low likelihood, the 10 CFR 50.59 evaluation does not need to consider the effects of the failure. Thus, the "qualitative assessment" provides a means of addressing potential failures to support a 10 CFR 50.59 evaluation.

2.2 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, the likelihood of failure may potentially increase. For redundant SSCs, this potential increase in the likelihood of failure may create an increase in the likelihood of a CCF.

The NRC has used the criteria from NEI 96-07, Revision 1, and NEI 01-01 in its discussions of "sufficiently low" threshold. These discussions are intended to clarify the existing 10 CFR 50.59 guidance; licensees should not interpret such discussions as a new or modified NRC position.

Criteria

For this RIS supplement, the outcome of the qualitative assessment is focused on a single likelihood threshold of "sufficiently low" that encompasses and satisfies the individual likelihood thresholds of 10 CFR 50.59(c)(2)(i), (ii), (v), and (vi). Although it may be required by other criteria, prior NRC approval is not required by10 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 the 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," 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 an SSC important to safety[2] 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 functions[3] (e.g., an increase in the 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 the occurrence of a malfunction of an SSC important to safety. Therefore, if the qualitative assessment outcome is "sufficiently low," 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," the activity does not introduce any failures 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, the 10 CFR 50.59 evaluation needs to consider the effects of this failure.

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

Does the activity create a possibility for a malfunction of an SSC that is 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 that "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 that is 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

---

2 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)."

3 The term "design functions," as used in this RIS supplement, conforms to the definition of "design functions" in NEI 96-07, Revision 1.

with the proposed activity is "sufficiently low," the activity does not introduce any failures 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 from any other 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, the 10 CFR 50.59 evaluation needs to consider the effects of this failure using methods consistent with the plant's UFSAR.

In some cases, the effects of a possible software CCF may not create a different result than any previously evaluated in the UFSAR.

3. Qualitative Assessments

The activities listed below are examples of digital I&C modifications that licensees can likely implement without prior NRC approval using properly documented qualitative assessments.

- replacement of analog relays (including timing relays) with digital relays
- replacement of analog controls for safety-related support systems such as chiller (heating, ventilation, and air conditioning) systems and lubricating oil coolers
- replacement of analog controls for emergency diesel generator supporting systems and auxiliary systems such as voltage regulation
- installation of circuit breakers that contain embedded digital devices
- replacement of analog recorders and indicators with digital recorders and indicators
- digital upgrades to non-safety related control systems

The evaluation of these proposed modifications is expected to be straightforward if they have no interconnectivity across channels, systems, and divisions; and they do not reduce the redundancy, diversity, separation, or independence[4] of their UFSAR-described design functions. However, digital modifications that involve networking, combining design functions from different systems; interconnectivity across channels, systems, and divisions; or shared resources merit careful review to ensure that such modifications incorporate appropriate design attributes so that reductions in the redundancy, diversity, separation, or independence of UFSAR-described design functions are not introduced.

Combining different design functions within digital modifications can result in combining design functions of different systems either directly in the same digital device or indirectly through shared resources, such as implementation of bidirectional digital communications or networks, common controllers, power supplies, or a multifunction display and control station. Shared resources (such as bidirectional communications, power supplies, controllers, and multifunction display and control stations) introduced by digital modifications may also reduce the redundancy, diversity, separation, or independence of UFSAR-described design functions.

[4] NEI 96-07, Section 4.3.2, explains that a change that reduces system/equipment redundancy, diversity, separation, or independence requires prior NRC approval because it would result in more than a minimal increase in the likelihood of occurrences of a malfunction of a SSC important to safety.

3.1 Qualitative Assessment Factors

Consistent with the guidance in NEI 01-01, this attachment specifies three general factors: (1) design attributes, (2) quality of the design process, and (3) operating experience. Qualitatively assessing and documenting these factors separately, and in the aggregate, will enable licensees to document qualitative assessments "in sufficient detail that an independent third party can verify the judgements." Note that design attributes and the quality of the design process are interrelated (i.e., the quality of the design process assures the proper implementation of design attributes). As a result, these two factors will always be essential elements of a qualitative assessment. Operating experience in most cases can serve to compensate for weakness in the other two factors. This guidance applies to modifications of safety-related systems or components but may also be applied to modifications of non-safety related systems or components at the discretion of the licensee.

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 the following:

> 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.

Design attributes of a proposed modification can prevent or limit failures from occurring. Design attributes focus primarily on built-in features such as fault detection and failure management schemes, internal redundancy, and diagnostics within the integrated software and hardware architecture. However, design features external to the proposed modification (e.g., mechanical stops on valves or pump speed limiters) may also 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 assessing the specific vulnerabilities through postulated failure modes (e.g., software CCF) within a proposed modification and applying specific deterministic design attributes to address those vulnerabilities (see Table 1). An adequate qualitative assessment of the likelihood of failure of a proposed modification would describe the potential failures that the proposed modification could introduce and the specific design attributes incorporated to resolve the identified potential failures. It would also explain how the chosen design attributes and features resolve the identified potential failures.

Diversity is one example of a design attribute that licensees can use to demonstrate that an SSC modified with digital technology is protected from a loss of design function caused by a potential CCF. In some cases, a plant's design basis may specify diversity as part of the design. In other cases, licensees do not need to consider the use of diversity in evaluating a proposed modification. Diversity within the proposed design can be a powerful means for significantly reducing the occurrence of failures that affect the accomplishment of design functions.

3.1.2 Quality of the Design Process

NEI 01-01, Section 5.3.3, states the following:

> 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.

Such processes include software development, hardware and software integration processes, system design, and validation and testing processes that have been incorporated into development. For safety-related digital equipment composed of integrated hardware and software, 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 digital equipment comprising integrated hardware and software, documentation of the development process may not be as extensive. 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.

The quality of the design process is a key element in determining the dependability of the proposed modifications. 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 (Std.) 1074-2006, "IEEE Standard for Developing a Software Project Life Cycle Process," which is 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 nonnuclear standards can also provide technically justifiable approaches for use if they apply to the specific application.

Quality standards should not be confused with quality assurance programs or procedures. Quality standards are those standards that 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 is a recognized standards development organization that publishes consensus-based quality standards that are relevant to digital I&C modifications. Quality standards used to ensure that a quality design process was used to develop the proposed change need not be limited to those endorsed by the NRC staff. The qualitative assessment document should demonstrate that the standard being applied is valid under the circumstances for which it is being used.

For non-safety related SSCs, adherence to generally accepted commercial standards may be sufficient. The qualitative assessment should list the generally accepted commercial industry standards used in development of the equipment. If NRC-endorsed industry standards were applied during the design or manufacturing process, or both, for non-safety related equipment, these standards may be documented in the qualitative assessment to provide additional evidence of quality.

3.1.3 Operating Experience

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

Relevant operating experience can be used to help evaluate and demonstrate that integrated software and hardware equipment employed in a propose modification has adequate dependability. The licensee may document information showing that the proposed system or component modification uses equipment with significant operating experience in nuclear power plant applications or in nonnuclear 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 and incorporation of lessons learned and document how that information demonstrates adequate equipment dependability.

Differences may exist in the specific digital I&C application between the proposed digital I&C modification and that of the integrated hardware 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 proposed system.

Further, the design conditions and modes of operation of the equipment whose operating experience is being referenced also need to be substantially similar to that of the proposed digital I&C modification. For example, analysts needs to understand the operating conditions (e.g., ambient environment, continuous duty) experienced by the referenced equipment and software. In addition, it is important to recognize that, when crediting operating experience from other facilities, one needs to understand which design features were present in the design whose operating experience is being credited. Design features that serve to prevent or limit possible CCFs in a design that is referenced as relevant operating experience should be documented 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 Factors Examples	
Factors	**Examples for Each Factor**
Design Attributes	• Defense-in-depth, diversity, independence, and redundancy (if applicable) • Inherent design features for integrated software and hardware or architectural/network (e.g., watchdog timers that operate independent of software, isolation devices, segmentation of distributed networks, self-testing, and self-diagnostic features) • Nonconcurrent triggers • Sufficiently simple (see NEI 01-01, Section 5.3.1) • Testability (e.g., highly testable) • Resolution of the possible failures identified in the failure analysis
Quality of the Design Process	Safety-Related Equipment: • Use of industry consensus standards shown to be applicable • Use of other standards shown to be applicable • Use of Appendix B vendors If an Appendix B vendor is not used, the analysis can state which generally accepted industrial quality program was applied. • Use of commercial-grade dedication processes in accordance with the guidance in EPRI TR-106439, “Guideline on Evaluation and Acceptance of Commercial-Grade Digital Equipment for Nuclear Safety Applications,” dated October 1, 1996. • Use of commercial-grade dedication processes in accordance with the guidance in Annex D to IEEE Std. 7-4.3.2, “IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations,” and with the examples in EPRI TR-107330, “ Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants” • Documented capability through qualification testing or analysis, or both, to withstand environmental conditions within which the SSC is credited to perform its design function (e.g., electromagnetic interference, radio-frequency interference, seismic activity) • Demonstrated dependability of custom software code for application software through extensive evaluation or testing Non-safety Related Equipment: • Adherence to generally accepted applicable commercial standards • Procurement or manufacturer documentation, or both, showing that design specifications are met or exceeded for equipment being replaced

	• Verification of design requirements and specifications
Operating Experience	• Operating experience in similar applications, operating environments, duty cycles, loading, and comparable configurations to that of the proposed modification • History of lessons learned from field experience addressed in the design • Referenced relevant operating experience should be equipment similar to that being proposed in the digital I&C modification. – Architecture of the referenced equipment and software (operating system and application) – Design conditions and modes of operation – Widely used high-quality commercial products with relevant operating experience used in other applications For software, limited use, custom, or user-configurable software applications can be challenging. – Experience with software development tools used to create configuration files

3.2 Qualitative Assessment Documentation

NEI 96-07, Revision 1, Section 5.0, and NEI 01-01, Appendix B, provide NRC-endorsed guidance for documenting 10 CFR 50.59 evaluations to meet the requirements of 10 CFR 50.59(d). 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 that support the 10 CFR 50.59 evaluation are subject to the aforementioned principles. For a knowledgeable reviewer to draw the same conclusion regarding qualitative assessments, the 10 CFR 50.59 evaluation documentation needs to include and clearly reference details of the considerations made and their separate and aggregate effects on any qualitative assessments. References to other documents should include the document name and location of the information within any referenced document (e.g., section or page numbers or both).

If qualitative assessment factors are used, the documentation would discuss each factor, including the positive and negative aspects considered, consistent with the examples provided in Table 1. In addition, the documentation would discuss the degree to which each of the categories was relied upon to reach the qualitative assessment conclusion.

4.0 Engineering Evaluations: Failure Analysis

Consistent with NEI 01-01, Sections 4.4.2 and 5.1, the failure analysis provides insights needed to determine whether the proposed change could reduce redundancy, diversity, separation, or independence, any of which is considered to result in more than a minimal increase in the likelihood of the occurrence of malfunctions. In addition to failures caused by software, it is

important to note that other effects of a digital modification could create new results of malfunctions (e.g., combining functions, creating new interactions with other systems, changing response time). The design should address these other effects. For example, if previously separate functions are combined in a single digital device, the failure analysis should consider whether single failures that could previously have affected only individual design functions can now affect multiple design functions. Where potential interconnectivity operational hazards are identified, the incorporation of appropriate design attributes should address these hazards. It is important to carefully document the analysis and resolution of potential operational hazards to ensure that future plant design changes appropriately address these hazards.

Section 4 of this RIS supplement is intended to emphasize key areas of consideration for identifying CCF vulnerabilities in the failure analysis to be addressed and documented in the final design and to support a qualitative assessment.

4.1 Failure Analysis

Failure analysis can be used to identify possible CCF vulnerabilities and assess the need to further modify the design. In some cases, design features and attributes could be used to preclude potential failures from further consideration. Modifications that use design attributes and features such as internal diversity or segmentation help to minimize the potential for CCFs. Similarly, backup capabilities offered by other systems can address identified failures. Sources of CCF vulnerabilities could include the introduction of identical software into redundant channels, the use of shared resources, or the use of common hardware and software across interconnected systems that perform different design functions. Another key consideration is that undesirable behaviors may not necessarily constitute an SSC failure but rather a misoperation (e.g., spurious actuation, erroneous control). Therefore, identifying sources of CCF to the extent practicable and addressing them during the design process is essential and constitutes an acceptable method for supporting the technical basis for the proposed modification.

Digital designs that have sources of CCF that could affect more than one SSC need to be closely reviewed to ensure that an accident of a different type or a malfunction with a different result 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 that use identical hardware and software, power supplies, or human-machine interfaces needs to be closely reviewed to ensure that possible common triggers have been addressed.

Unless the licensee's UFSAR already incorporates "best estimate" methods, it cannot use such methods to evaluate different results than those previously evaluated in the UFSAR. Use of "best estimate" methods in 10 CFR 50.59 evaluations is limited to the subject of the previous use of such methods in the UFSAR.

The failure analysis can also reveal potential sources of CCF introduced through software development and configuration tools. Careful consideration should also be given to individual programmable logic devices or user-configurable devices as potential sources of CCFs.

Digital Communications

Careful consideration should be given to digital communications to preclude effects on SSC independence within the failure analysis. Digital communications may introduce interactions resulting in new types of failure modes. Digital modifications that introduce digital networks, or interconnectivity across channels and divisions or between different systems should incorporate appropriate design attributes so that reductions in redundancy, diversity, separation, or independence of UFSAR-described design functions are not introduced. Adherence to applicable industry consensus standards (e.g., IEEE 7-4.3.2, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations") can provide technically justifiable design attributes to address potential failure modes of modifications with digital communications, including modifications to non-safety related SSCs.

Combining Design Functions and Shared Resources

Failure analysis may address the combination of design functions for different safety-related or non-safety related SSCs in a manner not previously evaluated or described in the UFSAR because such combinations could introduce new interdependencies and interactions that make identifying new potential failure modes more difficult. Of significant concern is the failure of combined design functions or within shared resources that (1) can affect malfunctions of SSCs or accidents evaluated in the UFSAR or (2) involve different defense-in-depth echelons.

Combining previously separate component functions can result in more dependable system performance because of the tightly coupled nature of the components and the reduction in complexity. If a licensee proposes to combine previously separate design functions or introduce shared resources in a safety-related or non-safety related digital I&C modification, it needs to carefully weigh possible new failures in relation to the benefits. Failure analysis and control system segmentation analysis can help identify potential issues. A segmentation analysis is particularly helpful for the evaluation of the design of non-safety related distributed networks.

Defense-in-Depth Analysis

The use of defense-in-depth design principles provides a means for addressing identified CCF vulnerabilities. NEI 01-01 describes the need for a defense-in-depth analysis as limited to substantial digital replacements of the reactor protection system and engineered safety features actuation system. However, a defense-in-depth analysis may be used to evaluate the capabilities of any digital modifications to reveal the impact of any new potential CCFs caused by 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, a 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 or procedures could serve to mitigate effects of possible CCF vulnerabilities introduced through the proposed modification.

4.2 Failure Analysis Resolution and Documentation

The licensee must develop and retain documentation for a proposed digital I&C modification in accordance with its NRC-approved quality assurance program. In doing so, the licensee will follow its design engineering procedures. The documentation of failure analysis identifies the possible vulnerabilities introduced in the design and the effects of failures resulting from such vulnerabilities. In addition, the documentation identifies the design features and procedures that resolve identified failures, as described in NEI 01-01, Section 5.1.4. The level of detail used should be commensurate with the safety significance and complexity of the modification in accordance with licensee procedures.

Licensees may, but need not, use the table in developing and documenting the failure analysis. Documentation should explain how adequate bases preclude or limit failures so that a knowledgeable reviewer could reach the same conclusion.

Table 2 Example: Failure Analysis Resolution and Documentation

Topical Area	Description
Step 1—Identification	• Describe the scope and boundaries of the proposed activity, including interconnections and commonalities with other SSCs. • List the UFSAR-described design function(s) affected by the proposed change. • Describe any new design functions performed by the modified design that were not part of the original design. • Describe any design functions eliminated from the modified design that were part of the original design. • Describe any previously separate design functions that were combined as part of the activity. • Describe any automatic actions to be transferred to manual control. • Describe any manual actions that are to be transferred to automatic control. • Describe the expected modes of operation and transitions from one mode of operation to another.
Step 2—Failure Mode Comparison	• Provide a comparison between the failure modes of the new digital equipment and the failure modes of the equipment being replaced. • If the failure modes are different, describe the resulting effect of equipment failure on the affected UFSAR-described design function(s). Consider the possibility that the proposed modification may have introduced potential failures: – Describe the effects of identified potential failure modes or undesirable behaviors, including, but not limited to, failure modes associated with hardware, software, combining

Table 2 Example: Failure Analysis Resolution and Documentation	
Topical Area	**Description**
	functions, use of shared resources, software tools, programmable logic devices, or common hardware/software. – Describe the potential sources of CCFs being introduced that are also subject to common triggering mechanisms with those of other SSCs that are not being modified. • Explain how identified potential failures are being resolved (see NEI 01-01, Section 5.1.4.).
Step 3—Determination of Equipment Dependability and CCF Likelihood	Based on the qualitative assessment factors provided in Table 1, is the new digital equipment at least as reliable as the equipment being replaced?
Step 4—Assessment of Equipment Dependability and CCF Likelihood Results	**IF** the results of Step 3 indicate that the new digital equipment is at least as dependable as the equipment being replaced or that the level of dependability is determined acceptable: • Document the bases for the conclusion. • Continue to Step 5. **IF** not, consider modifying the design or rely on existing design function backup capabilities.
Step 5—Documentation	Summarize the results and overall conclusions reached. Discuss the effect of the proposed activity, if any, on applicable UFSAR-described design functions. Discuss the differences in equipment failure modes and the associated effects of different failure modes on applicable UFSAR-described design functions. Describe the incorporation of design attributes to resolve potential CCF vulnerabilities. Examples of supporting documents include the following: • Applicable codes and standards applied in the design • Equipment environmental conditions (e.g., ambient temperature, electromagnetic interference, radio-frequency interference, seismic activity) • Quality design processes used (e.g., Subpart 2.7 of Part II of American National Standards Institute/American Society of Mechanical Engineers NQA-1, “Quality Assurance Program Requirements for Nuclear Power Plants”) • Commercial-grade dedication documentation, such as described in EPRI TR-106439 • Failure modes and effects analysis (if applicable) • Software hazard analysis (if applicable)

Table 2 Example: Failure Analysis Resolution and Documentation	
Topical Area	**Description**
	• Critical digital reviews, such as described in EPRI TR-1011710, "Handbook for Evaluating Critical Digital Equipment and Systems" (if applicable) • Documentation of equipment operating experience
Step 6—Application of Failure Analysis Conclusions to the 10 CFR 50.59 Evaluation Criteria	Apply engineering conclusions to the 10 CFR 50.59 evaluation questions.