The following document is a preliminary draft being made publically available to support a Category 3 public meeting on January 26, 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

DRAFT FOR DISCUSSION

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

January XX, 2018

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

DRAFT FOR DISCUSSION

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. This RIS Supplement clarifies the guidance for preparing and documenting "qualitative assessments" that licensees can use to develop written evaluations to address the criteria in 10 CFR 50.59, "Changes, tests and experiments." This RIS Supplement is intended to reduce regulatory uncertainty for licensees applying the 10 CFR 50.59 process and making digital I&C modifications without prior NRC approval. This RIS Supplement is not directed toward digital I&C upgrades and replacements of reactor

protection systems and engineered safety features actuation systems (ESFAS), since application of the guidance in this RIS Supplement to such changes would likely involve additional considerations. This RIS Supplement is also not intended to provide new design process guidance for addressing software common cause failure (software CCF) or methods for addressing common cause failure of the reactor protection systems and engineered safety features actuation systems. Specific guidance for addressing potential common cause failure of digital I&C equipment when making design changes to structures, systems, and components (SSCs) 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 this guidance in support of digital design modifications in conjunction with Regulatory Guide 1.187, "Guidance for Implementation of 10 CFR 50.59, Changes, Tests, and Experiments," dated November 2000 (ADAMS Accession No. ML003759710), which endorsed NEI 96-07, "Guidelines for 10 CFR 50.59 Implementation," Revision 1, dated November 2000 (ADAMS Accession No. ML003771157).

The regulations in 10 CFR 50.59(d)(1) state: "The licensee shall maintain records of changes in the facility, of changes in procedures, and of tests and experiments made pursuant to paragraph (c) of this section. These records must include a written evaluation which provides the bases for the determination that the change, test, or experiment does not require a license amendment pursuant to paragraph (c)(2) of this section."

The NRC inspections of documentation for digital I&C plant modifications prepared by some licensees using the guidance in NEI 01-01 uncovered inconsistencies in the performance and documentation of engineering evaluations of digital I&C modifications and inadequacies in the documentation of the technical bases supporting responses to the 10 CFR 50.59(c)(2) evaluation criteria. This RIS Supplement clarifies the RIS 2002-22 endorsement of the NEI 01-01 guidance by providing additional guidance for developing and documenting "qualitative assessments" adequate for use as bases for licensee evaluations addressing the criteria of 10 CFR 50.59(c)(2). In particular, this RIS Supplement clarifies the guidance for documenting licensee determinations that a digital modification will exhibit a "sufficiently low"[1]

[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).

DRAFT FOR DISCUSSION

likelihood of failure. This determination then serves as a technical basis supporting the conclusions that are reached when a licensee evaluates a proposed design against the criteria of 10 CFR 50.59(c)(2) to determine whether prior NRC staff approval is needed before the proposed design can be implemented.

In response to staff requirements memorandum (SRM)-SECY-16-0070 "Integrated Strategy to Modernize the Nuclear Regulatory Commission's Digital Instrumentation and Control Regulatory Infrastructure" (ADAMS Accession No. ML16299A157), NRC staff has engaged NEI and industry representatives to improve the guidance for applying 10 CFR 50.59 to digital I&C-related design modifications as part of a broader effort to modernize I&C regulatory infrastructure. The NRC staff's plan for accomplishing this update is outlined in the NRC's "Integrated Action Plan to Modernize Digital Instrumentation and Controls Regulatory Infrastructure" (ADAMS Accession No. ML17102B307). This plan, which is updated semiannually, provides a comprehensive view of NRC activities associated with improvements to the digital I&C regulatory infrastructure, including a planned schedule for completion of key regulatory infrastructure documents. In Section 5 of the NRC staff's Integrated Action Plan (IAP), the NRC staff outlines how it plans to clarify its previous endorsement of the NEI 01-01 guidance by providing additional guidance for developing and documenting acceptable qualitative assessments in support of the performance of 10 CFR 50.59 evaluations of proposed digital I&C modifications. Making available the guidance in this RIS Supplement is described as a near-term action in the IAP to provide specific guidance for documenting qualitative assessments that a proposed digital I&C modification will exhibit a sufficiently low likelihood of failure. The use of appropriately-prepared qualitative assessments is one acceptable way to document the evaluation of whether a design change can result in more than a minimal increase in the frequency of an accident or the likelihood of occurrence of a malfunction of an SSC important to safety previously evaluated in the final safety analysis report. The use of appropriately-prepared qualitative assessments is also one acceptable way to document the evaluation of whether a design change can result in accidents of a different type or malfunctions of SSCs with different results than previously evaluated. The assessment of such malfunctions includes the need to address the potential for common cause failures, (which is within the scope of the IAP), when proposing changes to SSCs that are of lesser importance to safety than that of reactor protection systems and Engineered Safety Features Actuation Systems. The IAP also describes a longer-term plan for incorporating the guidance of this RIS Supplement into durable guidance documents that are now under development. The NRC staff will continue to engage with stakeholders on the development of new guidance to address the identified issues and needs.

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 to 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 Sections 4, 5, and Appendix A of NEI 01-01. However, certain aspects of the guidance that discuss the relationship of 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).

DRAFT FOR DISCUSSION

SUMMARY OF ISSUE

Section 3.2.3 of the NRC staff's evaluation of NEI 01-01 (Attachment 1 to RIS 2002-22) states:

> The staff's position regarding documentation of 10 CFR 50.59 evaluations is accurately reflected in the second paragraph in Appendix A to the submittal, which states: "The 10 CFR 50.59 questions should be answered in sufficient detail, either by reference to a source document or by direct statements, that an independent third party can verify the judgements." The staff has reviewed Appendix A, "Supplemental Questions for Addressing 10 CFR 50.59 Evaluation Criteria," and Appendix B, "Outline for Documenting 10 CFR 50.59 Screens and Evaluations," and, based on the foregoing, concludes that the guidance therein is acceptable for licensees to use in performing and documenting their 10 CFR 50.59 evaluations.

This RIS Supplement emphasizes the staff's paragraph above.

Specifically, this RIS Supplement provides additional guidance on what is needed to ensure that licensees adequately perform and document "qualitative assessments" used to provide an adequate basis for a determination that a digital modification will exhibit a sufficiently low likelihood of failure, which is a key element in 10 CFR 50.59 evaluations of whether a change requires prior NRC approval. Digital hardware being introduced in a nuclear facility modification is typically expected to be more dependable than the equipment it is replacing. However, there are no established consensus methods for accurately quantifying the reliability of software. NEI 96-07 Revision 1, Section 4.2.1 states: "If a change has both positive and adverse effects, the change should be screened in. The 10 CFR 50.59 evaluation should focus on the adverse effects."

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, that can lead to the failure to perform a design function. 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 non-safety related control functions (e.g., controllers, communication networks or video display units), may include such a potential. The 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)]. The 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)]. NEI 01-01 describes that for 10 CFR 50.59 evaluations, the likelihood of failure is normally demonstrated qualitatively (i.e., through reference to reasonable engineering practices and engineering judgment), particularly for systems or components that rely on software, because there are no well-established, accepted quantitative methods to demonstrate the likelihood of failure from sources such as software design errors.

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

DRAFT FOR DISCUSSION

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 record 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, "Qualitative Assessment Framework," provides guidance for performing and documenting this qualitative assessment.

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

> Because there is currently no acceptable way to quantitatively establish the reliability of digital systems, [NEI 01-01] gives considerable attention to the qualitative assessment of the dependability of and risk associated with I&C systems. The guidance in the submittal [NEI 01-01] identifies qualitative approaches within existing endorsed guidance with regard to software issues, including software-related common-cause failure issues, without proposing alternatives to the existing guidance. Therefore, the guidance in [NEI 01-01] does not propose to alter, or offer less conservative guidance for, the existing licensing process for license amendment requests to implement digital replacements.

There is no change in NRC staff position regarding its endorsement of the guidance in NEI 01-01 for addressing digital I&C modifications under the 10 CFR 50.59 process. However, this RIS Supplement clarifies the staff's previous endorsement in RIS 2002-22 of the guidance in NEI 01-01 pertaining to the performance and documentation of adequate technical evaluations and adequately documented qualitative assessments to meet the requirements of 10 CFR 50.59. 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. The attachment to this RIS Supplement provides a framework for preparing and documenting qualitative assessments considered acceptable to serve as a technical basis supporting the responses to key 10 CFR 50.59(c)(2) evaluations.

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

NEI 01-01 supports the use of qualitative assessments, engineering judgment, and industry precedent when addressing whether frequency of occurrence of an accident or the likelihood of occurrence of a malfunction of an SSC important to safety would be more than minimally increased (evaluation criteria 10 CFR 50.59(c)(2)(i) and (ii)). NEI 01-01 also supports the use of such qualitative assessments when addressing whether a possibility for an accident of a different type or a malfunction of an SSC important to safety with a different result than any previously evaluated in the UFSAR would be created (evaluation criteria 10 CFR 50.59(c)(2)(v) and (vi)). This RIS Supplement describes the importance of documenting how the implementation of key design attributes, quality of the design processes, and an evaluation of relevant operating experience is being credited as the basis for making engineering judgments that the likelihood of failures of SSCs that are introduced by a proposed digital modification is low. Such qualitative assessments are used to provide an adequate basis for determining that the likelihood of failure for proposed modifications is low. The guidance in NEI 01-01 provides a "road map" to relevant standards and other sources of detailed guidance. The attachment to this RIS Supplement clarifies how the aggregate of the proposed digital I&C system design

DRAFT FOR DISCUSSION

features, quality of the design processes, and equipment and software operating experience that are applied to the proposed design using such standards and guidance can be documented by licensees when preparing qualitative assessments to support conclusions within a 10 CFR 50.59(c)(2) evaluation that a license amendment is not needed.

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

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

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. 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 the *Federal Register* on July 3, 2017 (82 FR 30913). The NRC received comments from 13 commenters. The NRC considered all comments, some of which resulted in changes to the RIS. The evaluation of these comments and the resulting changes to the RIS are discussed in a publicly-available memorandum that is available in ADAMS under Accession No. ML17296A852.

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.

DRAFT FOR DISCUSSION

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, NRO
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 Framework

DRAFT FOR DISCUSSION

Qualitative Assessment Framework

1. Purpose

Regulatory Issue Summary (RIS) 2002-22 provided the NRC staff's endorsement of Nuclear Energy Institute (NEI) Guidance document NEI 01-01, "Guideline on Licensing Digital Upgrades: EPRI TR-102348, Revision 1, NEI 01-01: A Revision of EPRI TR-102348 To Reflect Changes to the 10 CFR 50.59 Rule." 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 appropriate qualitative evidence available. 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. This RIS supplement guidance presumes that the qualitative assessment will be performed after all technical work (e.g. failure modes and effects analysis, and revised design documentation) is complete and that the proposed modification has already been determined to have a potential adverse effect (i.e. it has been 'screened in' as described in NEI 96-07).

If the "qualitative assessment" determines that a potential failure (e.g., software common cause failure [CCF]) has a sufficiently low likelihood, then the effects of this failure do not need to be considered in the 10 CFR 50.59 evaluation. In particular, this "qualitative assessment" provides a means of addressing software CCF.

This RIS Supplement includes guidance that licensees may use to develop adequate bases for determining that (1) a digital modification will exhibit a sufficiently low likelihood of failure, or, (2) if a digital I&C modification failure can be postulated, the effects of that failure will not result in a new type of accident or a malfunction of structures, systems, and components (SSCs) with different result than previously evaluated in the updated final safety analysis report (UFSAR). The determination of whether a modification will exhibit a sufficiently low likelihood of failure is a key element in 10 CFR 50.59. Licensees need to understand the possible effects of failures of a digital I&C modification to ensure that such effects will not create a possibility for an accident of a different type or a malfunction of an SSC with a different result than previously evaluated in the updated final safety analysis report.

The sections that follow provides one approach, acceptable to the NRC staff, for describing the scope, form, and content of a qualitative assessment.

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

After determining that an activity is safe and effective through appropriate engineering and technical evaluations, the 10 CFR 50.59 process is applied. 10 CFR 50.59 provides a threshold for regulatory review, not the final determination of safety, for the proposed activities. 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.

DRAFT FOR DISCUSSION

Evaluations must address all elements of proposed changes. Elements of a change can have positive effects on SSC failure likelihood while other elements of the change can 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.

When discussing 10 CFR 50.59 criteria, the words "met" or "satisfy" mean that a yes or affirmative answer has been achieved and an amendment is required.

2.1 Likelihood Justifications

Qualitative assessments are needed to document the bases to support a conclusion that a proposed digital I&C modification has a sufficiently low[2] likelihood of failure, consistent with the UFSAR analysis assumptions. This conclusion is used in the Title 10 of the *Code of Federal Regulations* (10 CFR) 50.59, "Changes tests and experiments," written evaluation to determine whether prior NRC approval is required.

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

The ability to provide an adequate basis for a determination that the digital modification will exhibit a sufficiently low likelihood of failure is a key element of 10 CFR 50.59 evaluations to determine whether the change requires prior NRC approval. To support the 10 CFR 50.59 process, methods are needed to evaluate the digital system likelihood of failure (e.g., based on the dependability of the modified digital components) that could result in a malfunction of an SSC important to safety. For digital equipment, however, there may not be well-established, accepted quantitative methods that can be used to estimate their dependability or likelihood of failure. Therefore, for digital SSCs, an adequate basis for determining sufficiently low likelihood of failure may be derived from a qualitative assessment of factors involving the inclusion of key system design features,[3] the quality of the design process used, and an evaluation of relevant operating experience (i.e., product maturity and in-service experience). The qualitative assessment reaches a conclusion through engineering judgment that there is an adequate basis for concluding that the digital modification will exhibit a sufficiently low likelihood of failure by considering the aggregate of these factors.

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 that the modification will exhibit a sufficiently low likelihood of failure. For digital modifications, particularly those that introduce software, there may be the potential increase in likelihood of failure, including a single failure.

DRAFT FOR DISCUSSION

[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).

[3] System design features are used to address anticipatable and quantifiable threats (e.g., the qualification of a piece of equipment to meet the plant seismic criteria ensures that the likelihood of failure from seismic event is sufficiently low). Defense-in-depth and diversity are system design features to address anticipatable but non-quantifiable threats (e.g., software CCF). These deterministic measures must be implemented under the appropriate quality processes.

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.

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, and the operating experience of the software and hardware used (i.e., product maturity and in-service experience). The qualitative assessment documents the factors, rationale, and reasoning for determining that the digital I&C modification exhibits a sufficiently low likelihood of failure by considering the aggregate of these factors.

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 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." 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). [Note: 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.]

Criteria

A qualitative assessment outcome of sufficiently low supports a no or negative answer for 10 CFR 50.59(c)(2)(i), (ii), (v), and (vi) as follows:
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 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

DRAFT FOR DISCUSSION

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 safety[4] 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 likelihood of failure of equipment that causes a failure of SSCs to perform their intended design functions (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 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 as likely to happen as those in the UFSAR." Accidents of a different type are caused by failures of equipment that initiate an accident of a different type. Only failures of equipment that are "as likely to happen as those in the UFSAR" can "create a possibility" of an accident of a different type. If the qualitative assessment outcome 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.

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 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. Only failures of equipment that are "as likely to happen as those in the UFSAR" can "create a possibility" of a malfunction

[4] 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 50, Appendix B)."

DRAFT FOR DISCUSSION

with a different result. If the qualitative assessment outcome 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.

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

The 10 CFR 50.59 evaluation of criterion (c)(2)(vi) can be viewed as a five-step process that stems from NEI 96-07, Revision 1, Section 4.3.6, which states: "The possible malfunctions with a different result are limited to those that are as likely to happen as those described in the UFSAR." This section provides excerpts from NEI 96-07, Revision 1, and NEI 01-01 and groups them into five steps to more clearly describe the considerations for addressing 10 CFR 50.59 criterion (c)(2)(vi). The section should not be interpreted as creating new or revised NRC positions:

Step 1: Develop a list of ways (i.e., failure modes of SSCs important to safety that are affected by the proposed modification) in which SSCs can fail to perform their intended design functions.

- "'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.)" [NEI 96-07, Rev. 1, Section 3.9, Definition of Malfunction of SSCs, page 18.]

Step 2: Perform a qualitative assessment of the likelihood of occurrence of each failure mode to determine which ones are as likely to happen as those described in the UFSAR.

- For digital systems, "reasonable assurance of adequate quality and low likelihood of failure is derived from a qualitative assessment of the design process and the system design features." [NEI 01-01, Section 5.3.1, page 5-14]

If the qualitative assessment outcome is not "sufficiently low," then perform Steps 3, 4, and 5 to evaluate the results of these failures against 10 CFR 50.59 criterion (c)(2)(vi).

Step 3: Determine the malfunction results.

- "The key issue is the effect of failures of the digital device on the system in which it is installed." [NEI 01-01, Section 4.4.6, page 4-19]

- "Another way to determine the appropriate level of detail is to consider the level at which design functions are described in the UFSAR. If the relevant design functions are assigned at the system level, then it is appropriate to evaluate the effects of malfunctions at this level." [NEI 01-01, Section 4.4.6, page 4-19]

- "If failures of the digital device cause the system to malfunction (i.e., not perform its design function), then the evaluation needs to determine if the result of the system malfunction is bounded by or different than those previously evaluated." [NEI 01-01, Section 4.4.6, page 4-19]

DRAFT FOR DISCUSSION

- NEI 01-01, Section 5.2, page 5-10 states that, "… reanalysis of design basis events is permitted using "best estimate" conditions and realistic assumptions…" Unless already incorporated into the design and licensing basis, "best-estimate" methods cannot be used for evaluating different results than those previously evaluated in the UFSAR. For failures in which likelihood is not "sufficiently low," the results of these failures are to be analyzed using methods consistent with the plant's design and licensing basis.

- "An example of a change that would create the possibility for a malfunction with a different result is a substantial modification or upgrade to control station alarms, controls, or displays that are associated with SSCs important to safety that creates a new or common cause failure that is not bounded by previous analyses or evaluations." [NEI 96-07, Section 4.3.1, page 55.]

- "If a feedwater control system is being upgraded from an analog to a digital system, new components may be added that could fail in ways other than the components in the original design. Provided the end result of the component or subsystem failure is the same as, or is bounded by, the results of malfunctions currently described in the UFSAR (i.e., failure to maximum demand, failure to minimum demand, failure as-is, etc.), then this upgrade would not create a "malfunction with a different result." [NEI 96-07, Section 4.3.6, page 54; also see NEI 01-01, Section 4.4.6, page 4-19.]

  "Note that [for criterion (vi)] new types of malfunctions are not the issue. NEI 96-07, Revision 1, states that 'a new failure mechanism is not a malfunction with a different result if the result or effect is the same as, or is bounded by, that previously evaluated in the UFSAR." [NEI 01-01, Section 4.4.6, page 4-19]

Step 4: Identify the associated malfunctions and results "previously evaluated in the UFSAR."

- "the evaluation needs to consider the level of detail that was previously evaluated in the UFSAR (i.e., component versus division/train versus system level failures)." [NEI 01-01, Section 4.4.6, page 4-19]

- "Another way to determine the appropriate level of detail is to consider the level at which design functions are described in the UFSAR. If the relevant design functions are assigned at the system level, then it is appropriate to evaluate the effects of malfunctions at this level." [NEI 01-01, Section 4.4.6, page 4-19]

Step 5: Compare the newly "created" results to the results of malfunctions "previously evaluated in the UFSAR." If the "created" results are not bounded by the previously evaluated results, then an LAR is required.

- "Once the malfunctions previously evaluated in the UFSAR and the results of these malfunctions have been determined, then the types and results of failure modes that the proposed activity could create are identified. Comparing the two lists can provide the answer to the criterion question." [NEI 96-07, Rev. 1, Section 4.3.6, page 55]

- "A new failure mechanism is not a malfunction with a different result if the result or effect is the same as, or is bounded by, that previously evaluated in the UFSAR." [NEI 01-01, Section 4.4.6, page 4-19]

DRAFT FOR DISCUSSION

3. Producing Qualitative Assessments that Support a Sufficiently Low Likelihood Conclusion

The qualitative assessment framework described herein may be used to develop and document the technical basis supporting a conclusion that a proposed digital modification satisfies each of the likelihood thresholds outlined above. The resulting qualitative assessments may then be used as part of the reasoning and rationale serving as the basis for a 10 CFR 50.59 evaluation. The NRC staff has determined that proposed digital I&C modifications having all the characteristics listed below are likely to result in qualitative assessment results that support a determination that a license amendment is not required by 10 CFR 50.59:

[Note: The term "design functions," as used in this RIS Supplement, conforms to the definition of "design functions" in NEI 96-07, Revision 1.]

1. Digital I&C design-functions replacing I&C design-functions 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, and
   b) Do not create a CCF vulnerability due to the incorporation of new shared resources (such as power supplies, controllers, and human-machine interfaces) with other design functions either explicitly (or implicitly) described in the final safety analysis report as updated (UFSAR) as functioning independently from other plant system functions, or modeled in the current design basis to be functioning independently from other plant design functions, and
   c) Do not affect reactor trip or engineered safety feature initiation/control logic design functions.

   "Integration," as used in this RIS clarification 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 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 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.

2. Digital I&C modifications to SSCs that do not result in a CCF vulnerability due to a reduction of any aspect of independence (or separation), single failure tolerance, or diversity credited in the UFSAR (including a reduction in diversity due to hardware or software resources shared among non-safety related control functions); and

3. Digital I&C modifications to facility SSCs, where a malfunction due to a design defect is precluded through: (a) simplicity (as demonstrated through 100 percent testing or a combination of testing and input/output state analysis); or (b) a demonstration of

DRAFT FOR DISCUSSION

adequate internal or external systematic diversity, or where a design defect is assumed, postulated to be triggered, and demonstrated to result in no new malfunction or a malfunction that is bounded at the level previously evaluated in the safety analysis.

Licensees may evaluate digital I&C modifications to SSCs associated with reactor protection systems and ESF actuation systems using the qualitative assessment clarification in this RIS Supplement with the following four considerations: (1) the proposed modification is not part of the actuation/control logic portion of reactor protection systems and ESF systems, (2) the proposed modification is not an extension of an ESF actuation, such as emergency power bus load sequencers, (3) the design function will continue to be accomplished and the proposed design will continue to satisfy applicable NRC requirements, and (4) any new input or output devices do not communicate with the actuation logic portion of reactor protection systems or ESF actuation systems using digital data communications. This would include possible changes to individual, non-shared channel inputs to reactor protection systems logic, reactor protection systems power supplies, or output actuators (relays/breakers). Proposed modifications beyond these types would likely require a license amendment.

4. Qualitative Assessment

4.1. Quantitative vs. Qualitative

A quantitative assessment is one capable of representing the SSC by a mathematical model, such as apportioning the reliability and availability goals among parts of the system, assigning probabilities to each failure mode of concern, and reconciling the calculated estimates of reliability and availability with the overall SSC goals. A qualitative assessment identifies possible ways in which an SSC can fail, and identifies appropriate precautions (design changes, administrative procedures, etc.) that will reduce the frequency or consequences of such failures. For example, a licensee may be able to rely on a qualitative assessment of a particular digital controller even if it is difficult to demonstrate that the controller uses an error-free operating system and error-free application-specific system software logic commands. Specifically, it may be possible to demonstrate qualitatively that the controller has a set of specific attributes that allow its installation without prior NRC approval. One acceptable set of attributes is that (1) software for that controller has been prepared using a high-quality software development process, (2) the controller was tested thoroughly during acceptance and post-installation tests, and (3) the particular controller has been used in tens of thousands of hours of successful operation at other locations under similar plant conditions and for similar purposes, and there has been no evidence of operational failures due to software defects.

The qualitative assessment conclusion makes use of engineering judgment. As stated above, NEI 01-01 describes that for 10 CFR 50.59 evaluations, the likelihood of failure is normally demonstrated qualitatively (i.e., through reference to reasonable engineering practices and engineering judgment) particularly for systems or components that rely on software, because there are no well-established, accepted quantitative methods to demonstrate the likelihood of failure from software design errors. When applying engineering judgment, the following principles and general considerations may be followed:

- The technical qualifications of the personnel performing such evaluations will be appropriate for the evaluation preparation and reviews.
- The evaluation process follows the applicable corporate engineering or plant engineering procedures for performing such engineering evaluations or calculations.

DRAFT FOR DISCUSSION

- The basis for conclusions relying on engineering judgment are clearly documented in the evaluation/analysis.
- A sound technical basis or rationale for the judgment (e.g., recognized engineering principles, standards, trend evaluations, and empirical data; previous engineering experience, calculations, or evaluations; demonstrated industry practices, etc.) is established.
- The level of detail used to justify the engineering judgment may be commensurate with the safety significance and complexity of the design function affected in accordance with licensee's procedures.
- The level of detail permits another technical reviewer with similar expertise, and without recourse to the author, to understand the author's rationale.
- Simplified models and estimation techniques can provide supporting bases for engineering judgement.

4.2. Overview of Design Information that Supports Qualitative Assessments

Technical information is needed to support a conclusion that a proposed digital I&C modification will exhibit a sufficiently low likelihood of failure. As described in greater detail below, an adequate basis for determining sufficiently low likelihood of failure may be derived from a qualitative assessment of factors involving the inclusion of key system design features, the quality of the design process used, and an evaluation of relevant operating experience (i.e., product maturity and in-service experience). The qualitative assessment reaches a conclusion through engineering judgment that there is an adequate basis for concluding that the digital modification will exhibit a sufficiently low likelihood of failure by considering the aggregate of these factors. Section 5 of this Attachment provides further discussion regarding technical information supporting qualitative assessments.

4.3. Qualitative Assessment Categories

Consistent with the guidance provided in NEI 01-01, this attachment specifies three general categories of proposed design-related characteristics (described in Table 1 of this document) that can be used to develop justifications that demonstrate a sufficiently low likelihood of failure for a proposed modification. The aggregate of the three qualitative assessment categories form the technical basis for developing justifications based upon the likelihood of failure (i.e., single failures and CCF) of a digital I&C modification to a system or components. The aggregate of all three categories below needs to be evaluated to demonstrate that there is an adequate basis for concluding that the proposed modification will exhibit a sufficiently low likelihood of failure such that the criteria described in Section 2 of this attachment can be addressed:

- Design attributes:

  NEI 01-01 Section 5.3.1 states:

  > To determine whether a digital system is sufficiently dependable, and therefore that the likelihood of failure is sufficiently low, there are some important characteristics that should be evaluated. These characteristics, discussed in more detail in the following sections include". . .

DRAFT FOR DISCUSSION

> Hardware and software design features that contribute to high dependability (See Section 5.3.4)." Such [hardware and software design] features include built-in fault detection and failure management schemes, internal redundancy and diagnostics, and use of software and hardware architectures designed to minimize failure consequences and facilitate problem diagnosis.

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

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, etc.) with the potential negative effects (e.g., software CCF, etc.).

Within the concept of defense-in-depth, acceptable justification for concluding an accident of a different type will not be initiated could include, if supported by the facts, that the postulated new accident is only possible after a sequence of multiple unlikely independent failures. This type of justification is summarized and documented as part of the qualitative assessment.

- 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. Although in many cases this development process would be documented and available for referencing in the qualitative assessment for proposed modifications to safety-related equipment, for commercial- grade-dedicated or non-safety related equipment it 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.

DRAFT FOR DISCUSSION

- 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 as a means 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.

These categories are not mutually exclusive and may overlap in certain areas. Adequate qualitative assessments for SSCs fully address each of the above categories. Qualitative assessment documentation for the proposed modification to SSCs is retained in accordance with the licensee's design engineering procedures, procedures implementing 10 CFR 50.59(d)(1), and NRC-approved QA program.

Table 1 provides acceptable examples of design attributes, quality of the design processes, and documentation of operating experience. This listing is not all inclusive, it merely provides examples. Licensees may consider additional design attributes, quality of the design processes, and documentation of operating experience in their qualitative assessment and need not use these specific examples.

DRAFT FOR DISCUSSION

Table 1—Qualitative Assessment Category Examples	
Categories	Acceptable Examples for Each Category
Design Attributes	• Design criteria—Diversity (if applicable), Independence, and Redundancy. • Inherent design features for software, hardware or architectural/network— Watchdog timers that operate independent of software, isolation devices, segmentation, self-testing, and self-diagnostic features. • Basis for identifying that possible triggers are non-concurrent. • Sufficiently simple (i.e., enabling 100 percent testing or comprehensive testing in combination with analysis of likelihood of occurrence of input/output states not tested). • Unlikely series of events—Evaluation of a given digital I&C modification would necessarily have to postulate multiple independent random failures in order to arrive at a state in which a CCF is possible. • Failure state always known to be safe, or at least the same state as allowed by the previously installed equipment safety analysis.
Quality of the Design Process	• Justification for use of industry consensus standards—for codes and standards not endorsed by the NRC. • Justification for use of the other standards. • Justification for applicability of standards used. • 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-107339. • Demonstrated tolerance (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.) • The use of custom software using code for application software will typically call for extensive evaluation or testing or both to demonstrate dependability, where there is inadequate information to conclude that a quality design process has been used.
Operating Experience	• 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 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.

DRAFT FOR DISCUSSION

	• 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. • Evaluation of the operating experience for specific versions of operating system software designed by high quality commercial grade equipment vendors may be one of the only means by which a degree of assurance of reliability may be judged. For some applications and custom-developed software, operating experience may be the most reliable justification that the software is acceptable. It may be necessary to delay implementing major application software use and software revisions until the software version has sufficient operating experience. • The operating system and application level software may need to be considered. In some cases it may be necessary to address vendor software that creates the configuration files as well as the configuration file itself.

4.3.1 Design Attributes to Reduce the Likelihood of Failure

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 the introduction of failure modes (e.g., software CCF) within a proposed modification and applying specific design attributes to address those vulnerabilities (see Table 1 above). An adequate qualitative justification regarding the likelihood of failure of a proposed modification would consist of a description of: (a) the identified vulnerabilities of the proposed modification, (b) the design attributes used to address the identified vulnerabilities, and (c) a clear description explaining why the chosen design attributes and features are adequate.

Changes in control system design need to be evaluated for potential vulnerabilities to CCF. In addition, there are some SSCs that have few applicable requirements (e.g. no diversity or redundancy requirements). These SSCs may have been implemented in a manner (i.e., relatively independently) such that only individual SSC malfunctions or failures were considered in the UFSAR. If these individual SSCs are combined with (e.g., controlled by a common digital component, employ the same software in separate digital devices), or are coupled to each other (e.g., by digital communication), then the potential for malfunctions with a different result or accidents of a different type would be evaluated under 10 CFR 50.59.

4.3.1.1 Diversity and Common Cause Failure

Diversity is one example of a design attribute of an SSC that can be used as part of the bases for demonstrating an SSC modified with digital technology will exhibit a low likelihood of a loss of design function due to a potential common cause failure. The design of certain SSCs is required to include diversity to the extent practical. (For example, for protection systems, "diversity is to be used to the extent practical to prevent loss of the protection function." (10 CFR Part 50 Appendix A, Criterion 22.)). Some licensees have already followed staff guidance, such as NUREG-0800, Chapter 7, Branch Technical Position 7-19, in establishing the

DRAFT FOR DISCUSSION

design basis of certain SSCs. Further, some SSCs are subject to existing regulatory requirements or other acceptance criteria to which the licensee is committed, and include diversity in the design. In these cases, the licensees have incorporated diversity into the design basis. In all other cases, the licensees need not consider the use of diversity (i.e., as described in the staff requirements memorandum on SECY 93-087) in evaluating a proposed modification under 10 CFR 50.59. However, diversity within the proposed design, and any affected SSCs is a powerful means which may significantly reduce the likelihood of malfunctions affecting the accomplishment of design functions.

4.3.1.2 Digital Communications

Digital communications can reduce SSC independence credited or assumed in the UFSAR. Reduction in independence may create the possibility of a new failure that could result in concurrent failures not considered in the UFSAR. Careful consideration is needed to preclude adverse effects on safety and non-safety related SSC independence. DI&C-ISG-04, Revision 1, "Highly-Integrated Control Rooms—Communications Issues" (ADAMS Accession Number ML083310185) provides an acceptable means of addressing digital communication between redundant SSCs, echelons of defense-in-depth, or SSCs with different safety classifications. DI&C-ISG-04 was developed to address digital communication among safety-related and between safety-related and non-safety related SSCs. The principles of this ISG or other technically justifiable considerations, may be used to assess non-safety related SSCs.

4.3.1.3 Combining (Integration) of 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 (i.e., single failures and CCF). 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[5]; 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 such a combination does not create a new failure mode, it is generally acceptable. In all cases in which a licensee proposes to combine previously separate design functions in a safety-related and/or non-safety related digital I&C, the qualitative assessment needs to weigh the risks of possible new malfunctions against the benefits of combining the previously separately controlled functions. Where possible, failure modes and effects analyses and non-safety related control system segmentation analyses can be performed for the proposed modification.

4.3.2 Quality of the Design Process and the use of Quality Standards

DRAFT FOR DISCUSSION

[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.

Quality of the design process is a key element that determines the dependability of proposed modifications. Licensees employing design processes consistent with the requirements of their NRC approved quality assurance program 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 IEEE Std. 1074-2006, "IEEE Standard for Developing a Software Project Life Cycle Process," RG 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.

4.3.3 Evaluation of Relevant Operating Experience

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, 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, and what operating conditions (e.g., ambient environment, continuous duty, etc.) were experienced by the referenced design. Design features, which serve to prevent or limit possible common cause failures, and references into relevant operating experience, should be noted, and considered 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.

5. Engineering Evaluations Supporting Qualitative Assessments

5.1 Introduction

This section describes approaches that could be used for conducting and documenting engineering evaluations when they are used to support qualitative assessments. In some cases

DRAFT FOR DISCUSSION

these approaches describe efforts beyond those discussed in NEI 01-01. This information is provided for consideration only. They do not represent an NRC position of what is necessary or required. Use of any of this information is at the discretion of licensees.

Prior to implementing new digital I&C designs, engineering evaluations of the proposed design need to be performed as part of the design and verification processes. Although the plant is designed to cope with single failures of SSCs, it is possible that new sources of common cause failure could be introduced as part of the digital I&C design, such as through the introduction of identical software into redundant channels; through the use of shared resources; or common hardware and software among systems performing different design functions. Therefore it is essential that such sources of common cause failure be identified, to the extent practicable, and addressed during the design stage as one acceptable method to support the technical basis concluding that a proposed new design has a low likelihood of failure that is evaluated in the subsequent licensing evaluation.

Section 3.2.2 of NEI 01-01 states:

> For digital systems, the likelihood of software-related failure is minimized using the same basic approach of controlling the design, implementation, operation, and maintenance processes. Compliance with industry standards and regulatory requirements coupled with tests, evaluations, and reviews is used to assure a very low likelihood of failure. The important activities that are performed throughout the various phases of the digital modification process and that contribute to minimizing risk are summarized in Section 3.3 ["Phases of the Plant Modification Process"] and discussed in detail in Section 5 ["Additional Guidance on Addressing Digital Upgrade Issues."] Results of these activities are then used in the 10 CFR 50.59 process as described in Section 4 ["Licensing Process and 10 CFR 50.59."] With respect to failures due to software, including common cause failures, *the key to addressing these in licensing is having performed appropriate design, analysis and evaluation activities to provide reasonable assurance that such failures have a very low likelihood."* [*emphasis* added]

Such key evaluation activities may include, but are not limited to: a) the deterministic analysis of the conformance of the design with regulatory requirements, engineering standards, and regulatory guidance, as well as the licensing basis of the plant; b) the performance of adequate deterministic failure analyses, including analysis of the effects of digital I&C failures at the component-level, system-level, and plant-level; c) the evaluation of the proposed modification for its overall "dependability"; and d) the deterministic evaluation of the design for the adequacy of its ability to provide adequate defense-in-depth. It should be noted that items b), c), & d) may be distinct analyses from a), but they are performed as a consequence of a). The qualitative assessment framework discussed in the previous sections of this Attachment relies, in part, on the technical bases and conclusions documented within these engineering evaluations.

Design Process Considerations

Section 3.2 of NEI 01-01 includes a figure (Figure 3-2, "Using Failure Analysis to Understand and Manage Risk") that illustrates "how failure analysis is applied during the design process to understand and manage risk. Risk is a function of both the likelihood and the consequences of potential failures and hazards. Depending on the combination, risk could be judged to be negligible, non-negligible (but acceptable), or unacceptable. *In practice, the design process*

DRAFT FOR DISCUSSION

identifies unacceptable risks and makes adjustments accordingly, so by the time a proposed change is ready for implementation in the plant or for NRC review, it will always lie in the region of negligible or acceptable risk." [*emphasis* added]

The design process, in part, answers the following questions: a) what can go wrong? b) how likely is it to occur?; and c) what actions are needed to address it? In Section 5.2, key engineering evaluations are described that provide insights to whether adequate design attributes and features have been incorporated to minimize the occurrence of system failures, and to demonstrate sufficient system/equipment redundancy, diversity, separation, or independence.

Section 3.1 of NEI 01-01 states:

> Engineering evaluations include the collection of activities that are performed to demonstrate reasonable assurance that the system is safe and satisfies the specified requirements (e.g., for quality, dependability, and performance). This may include evaluating and interpreting the results of the failure analysis, design verifications, software V&V, and review of vendor software design and development processes. Where appropriate, analyses of overall defense-in-depth and diversity of the plant may be warranted to demonstrate the ability to cope with common cause failures.

Section 4.1.1 of NEI 01-01 states that two key elements of the engineering evaluations are evaluating the dependability of the digital equipment and its associated software, and analyzing potential failures. "One of the key considerations in licensing digital upgrades is determining whether failures due to software are as likely as other potential failures addressed in the UFSAR. This issue is addressed by establishing reasonable assurance that such failures are unlikely, based on the engineering evaluations performed as part of the design process."

5.2 Key Engineering Evaluations

Section 4 "Engineering Evaluations" of Appendix B, "Outline for Documenting 10 CFR 50.59 Screens and Evaluations," of NEI 01-01 provides guidance for documenting why the proposed digital I&C modification as designed is considered appropriate for the application. This Appendix section describes types of engineering evaluations that may be used to provide justification as to why the proposed design is appropriate. These include an evaluation of the design for conformance with applicable design criteria, regulatory requirements and industry standards.

The analyses described below represent acceptable methods for performing engineering evaluations supporting a qualitative assessment. 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 software CCF, reduce the likelihood of occurrence of a possible software CCF, or mitigate the effects of a software CCF that can occur.

5.2.1 Failure Analyses

DRAFT FOR DISCUSSION

As stated in Section 5.1 of NEI 01-01, a digital I&C modification failure analysis is a part of the design process that "should be performed as part of plant design procedures and should be documented as part of the design process." The performance of such a deterministic failure analysis of a proposed digital I&C modification is one acceptable method for providing insights regarding the possible failure modes of the modification that are needed to support such licensing evaluations, which are typically performed later in the modification process. The failure analysis provides, in part, the insights needed to determine if a proposed digital I&C modification is vulnerable to possible software CCF such that the resulting design could reduce redundancy, diversity, separation, or independence, which could result in more than a minimal increase in the likelihood of occurrence of accidents or malfunctions. Such deterministic failure analyses provide feedback to the designers regarding effects of possible failures of the proposed digital I&C modification on plant systems so that the designers can make determinations as to whether there is a need to further modify the design to address any design issues that are uncovered. For example, a failure analysis may reveal that due to the adequacy of design features already included within a proposed design, the possible occurrence of failures due to a software CCF vulnerability is considered to have such a low risk that the proposed design is considered to be adequate.

NEI 01-01 Section 5.1 states, in part, that the "failure analysis should include the following elements..:"

- Identification of potential system-level failure and undesirable behavior (which may not be technically "failures") and their consequences. This includes consideration of potential single failures as well as plausible common cause failures.

- Identification of potential vulnerabilities, which could lead to system failures or undesirable conditions.

- Assessment of the significance and risk of identified vulnerabilities.

- Identification of appropriate resolutions for identified vulnerabilities, including provide [sic] means for annunciating system failures to the operator.

NEI 01-01 Section 5.1 also states:

> A variety of methodologies and analysis techniques can be used in these evaluations, and the scope of the evaluations performed and documentation produced depends on the scope and complexity of the upgrade. The analysis maintains a focus at the level of the design functions performed by the system, because it is the effects of the failure on the system and the resulting impact on the plant that are important. Failures that impact plant safety are those that could: prevent performance of a safety function of the system, affect the ability of other systems to perform their safety functions, or lead to plant trips or transients that could challenge safety systems.

NEI 01-01 Section 5.1.1 states, in part,

DRAFT FOR DISCUSSION

> It is useful at this stage to review the UFSAR to determine how failures of the affected system are described and analyzed. An understanding of the UFSAR-described failures and their results is needed to support the 10 CFR 50.59 evaluation discussed in Section 4 ["Licensing Process and 10 CFR 50.59."] If the plant design change introduces any failures that cause results different from those analyzed in the UFSAR, then a license amendment may be required.

The introduction of new digital designs having sources of CCF in common with other plant non-safety related designs that have been assumed in the safety analyses to remain functional, may result in the plant being put into a condition for which it has not been analyzed. This is particularly the case when such common sources of CCF also are subject to common triggers.

An adequate failure analysis is one that includes a sufficient level of detail to enable licensees to make a determination as to the possibility for and likelihood of potential new failures that could be introduced by a proposed modification. This includes an understanding of the operations of any external connections of the modified SSC(s) to and from other SSCs, as well as an understanding of how identical hardware and software, power supplies, human-machine interfaces, etc. may have been employed elsewhere in the plant, such that after the modification has been implemented, there remains a possible commonality in vulnerabilities to the same common cause sources and their triggers. NEI 01-01, Section 4.1.2 states that additional factors that can contribute to the determination that the likelihood of software CCF is acceptably low include:

> Simple software architecture, few inputs/outputs, well-defined failure states, built-in fault tolerance (see Section 5.3.2). Systems that are sufficiently simple can have well defined failure modes and tend to allow for more thorough testing of all input and output combinations than complex systems. The simplicity of the digital equipment itself and of the application should be considered.

Modifications that employ effective design attributes and features such as internal or external systematic diversity help to ensure that possible vulnerabilities do not result in CCFs. The design of such systems are deemed to be adequate.

5.2.2 Dependability Evaluation

The "dependability" of a design is described in NEI 01-01 (Page 2-3) as "a broad concept incorporating various characteristics of digital equipment, including reliability, safety, availability, maintainability, and others." Section 4.1.2 of NEI 01-01 states:

> To determine whether a digital system poses a significant risk of software failure, the factors that contribute to its dependability (or likelihood of failure) and quality need to be evaluated.

NEI 01-01, Section 4.1.2 further states that additional factors that can contribute to the determination that the likelihood of software CCF is acceptably low include:

> The maturity of the product and substantial relevant history of satisfactory operation in similar application (including operating experience at other plants and in other industries). Additional confidence is gained if the same equipment

DRAFT FOR DISCUSSION

and application program have been used successfully in other nuclear plants or other similar applications.

Technical evaluation in combination with deterministic design measures can be used to make a determination as to whether a proposed I&C modification is "sufficiently dependable." However, there might not be clearly applicable consensus methods for accurately quantifying the reliability of software. Therefore, it may be necessary to use "engineering judgment" as to whether the proposed design is still "sufficiently dependable" in its ability to perform its required functions while significantly limiting, or avoiding the introduction of possible new sources of software CCF.

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, staff believes that judgements 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 vulnerabilities to software 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 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…." It may be challenging to demonstrate "sufficient dependability" using solely the quality of the design process.

5.2.3 Defense-in-Depth Analyses

If there are specific licensing basis discussions for diversity or defense-in-depth applicable to the affected design function they must be explicitly addressed. For example, as discussed in Section 5.2 of NEI 01-01, a "defense-in-depth and diversity" (D3) analysis is required when the trip logic and actuation portions of the RTS and/or ESFAS are modified with digital equipment.

Although a formal D3 analysis is not required for non-protection systems, a defense-in-depth analysis should also be considered for complex digital modifications of non-protection systems to determine the impact of any new potential vulnerabilities to common cause failures 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. If a new potential common cause vulnerability has been introduced, the defense in depth analysis can identify whether there may be diverse manual or automatic means that can perform the same or different functions or whether additional design features (e.g., internal diversity) are appropriate for incorporation.

Possible software CCFs that have been identified in the failure analysis (and not eliminated from consideration based on the dependability evaluation) can be assessed to determine whether

DRAFT FOR DISCUSSION

adequate diversity and defense-in-depth will remain after the digital I&C modification is implemented. Possible means, for ensuring adequate diversity and defense-in-depth will remain at the system or plant level, can include: (a) the use of design attributes to achieve adequate diversity, (b) the crediting of available high-quality, non-safety related, but independent systems, or (c) manual actions that are already analyzed and credited in the UFSAR safety analysis.

DRAFT FOR DISCUSSION

Section 5.2.1 of NEI 01-01 states:

> The cumulative effects of a series of upgrades or modifications should also be considered in the determination of whether a defense-in-depth and diversity analysis is performed. For any change to the plant, consideration should be given to the effects the change may have on diversity and defense-in-depth for RTS/ESFAS functions. If the change would affect the diversity and defense-in-depth of the RTS/ESFAS functions, then the analysis should be performed.
>
> Also, if other I&C systems, including ATWS and other non-safety systems, are being upgraded to digital in plants where digital upgrades to RTS and/or ESFAS have already been done, prior defense-in-depth and diversity analyses should be reviewed. If the I&C system under consideration was credited in the prior analysis as providing backup, then the replacement digital equipment should be diverse from that used in the protection systems. NUREG-6303 provides guidance on methods that can be used to assess the diversity of digital systems.

For RPS and ESFAS, BTP 7-19, Revision 7, Section 1.9 states that many system design attributes, testing, procedures, and practices can contribute to significantly reducing the probability of CCF occurrence. "However, there are two design attributes, either of which is sufficient to eliminate consideration of software based or software logic based CCF." For other systems, different design attributes and testing can be used if: (1) technically acceptable, (2) suitable for the application, and (3) defensible. Properly implemented, these different attributes could serve to significantly reduce uncertainty and establish that the risk is determined negligible or acceptable.

To simplify and to facilitate the D3 analysis, a CCF may be assessed using best-estimate methods and realistic assumptions. However, such methods are not appropriate for use in evaluating the effects of failures when performing 50.59 evaluations. Unless already incorporated into the design and licensing basis, "best-estimate" methods cannot be used for evaluating different results than those previously evaluated in the UFSAR.

A defense-in-depth evaluation may reveal any direct or indirect impacts on interfaces with existing plant SSCs. This type of evaluation may reveal there are existing backup capabilities that could serve to mitigate any negative effects of possible low likelihood failures that could be introduced through the proposed design of the modification.

5.3 Appropriate Resolution to Identified Failures

If a postulated common cause failure of a digital modification has been provisionally determined to be not sufficiently low, in general, the following options can be considered:

- seek NRC approval first, pursuant 10 CFR 50.90 for the modification;
- satisfy 10 CFR 50.59 criteria using an alternative approach[6]; or
- redesign the proposed modification so that a sufficiently low likelihood of failure conclusion could be made.

[6] An example of an alternative approach is a deterministic conclusion that failure likelihood is less than comparable failures in the UFSAR.

DRAFT FOR DISCUSSION

NEI 01-01 Section 5.1.4, states, in part, with regard to appropriate resolution for identified potential failures, the following:

> Modify the design or apply greater emphasis to appropriate parts of the design process to address the potential failure. If the failure is considered significant because of a lack of confidence (or difficulty in achieving reasonable assurance) in a portion of the design or in a particular software element in the design, then one option may be to apply additional design verification or testing activities. This additional design verification or testing could develop the needed confidence and achieve reasonable assurance that the likelihood of the failure is such that it is no longer considered a significant risk [sufficiently low]. Alternatively, the design itself may be modified to either preclude the failure (e.g., make it fail safe for this particular failure) or add internal backups in the design, such as redundancy or diversity.

Redesigning a proposed modification to include additional design attributes, design features (e.g., internal or external systematic diversity) and/or additional design verification and testing activities is a recommended option for licensees to consider if the licensee wants to implement the modification without prior NRC approval. Redesigning could also help ensure potential new failure modes and misbehaviors are adequately addressed in the design. Providing additional design verification and/or testing activities on software or software-based elements of a proposed design that demonstrates high reliability can be a key consideration in demonstrating the overall dependability of the proposed modification and that the modification will exhibit a low likelihood of failure.

NEI 01-01 Section 5.1.4, also states, in part, with regard to appropriate resolution for identified potential failures, the following:

> Rely on existing backup capability offered by existing systems to address the failure – other equipment or systems that provide alternate ways of accomplishing the function or otherwise provide backup for this failure. This may include operator action if there is adequate information and time available for the operator to act, and with appropriate procedures and/or training.
>
> Supplement the existing backup capability such that the failure is adequately addressed. This could include improving the ability to detect the failure automatically so the repair response will be timely, improving procedures and training for the operators to mitigate the effects of the failure, or providing additional backup capability (e.g., manually operated switches for critical functions and procedural guidance for their use), so that the resulting risk is insignificant.

Reliance on existing backup capability that has been evaluated and documented as part of a plant's licensing bases is one acceptable means to address postulated failure modes and undesirable behaviors of a proposed digital I&C modification. Similarly, re-design of existing backup capabilities is also considered acceptable, as a means to address failures that can be introduced by the modification. In cases where reliance on back-up capability or operator actions is not part of the plant's licensing basis, prior NRC approval would likely be required.

DRAFT FOR DISCUSSION

5.4 Documentation of Engineering Evaluations

The documentation of adequate engineering evaluation outlines the identification of potential new failure modes or undesirable behaviors on the design function of the modified SSC(s) or other SSC(s), the possible effects of these vulnerabilities on plant safety, and the design features or operating provisions that are being put into place to prevent and/or mitigate their occurrence as well as descriptions of the types of engineering evaluations performed. Documenting an adequate engineering evaluation of appropriate resolutions to the identified vulnerabilities permits a clear understanding by designers and future evaluators of the potential effects of the vulnerabilities to plant safety and operations.

Table 2 below provides a suggested outline for documentation to support NEI 01-01 Appendix B guidance for engineering evaluations that supports and forms the basis for qualitative assessments for safety-related and non-safety related SSCs, as applicable. Although not required, licensees may use Table 2 as an example basis for the level of detail, types of evaluations, and documentation such that technical conclusions reached through the engineering evaluations can be verified independently. Implementation details are at the discretion of the licensee, consistent with the licensee's procedures.

Engineering Evaluations and Documentation for Non-Safety Related SSCs

With regard to engineering evaluations of non-safety related SSCs, there may be differences in the level of detail, types of analyses and documentation based upon the non-safety related SSC(s) being modified and the characteristics of the design within the proposed modification.

Adequate engineering evaluation for non-safety related SSCs helps ensure:

- Postulated new failure modes do not result in concurrent failures in shared resources, common hardware and software, or communications among two or more different non-safety related SSCs such as the combining of different design functions that were previously separate (e.g. Feedwater and Turbine Bypass controls).

- Postulated new failure modes do not exist that could propagate to two or more different non-safety related SSCs such that the effect could place the plant into an unanalyzed condition based upon the plant's existing safety analysis.

- Identified vulnerabilities have been adequately addressed (e.g. specific design features, quality of the design processes or demonstration of relevant operating experience).

Documentation for non-safety related modifications should be consistent with the licensee's procedures. Licensees need not prepare formal qualitative assessments for every proposed digital modification to non-safety related SSCs where the nature of the proposed modification does not have the characteristics described above (i.e., with the potential to impact assumptions in the safety analysis), consistent with requirements of licensee procedures.

DRAFT FOR DISCUSSION

Table 2—Example - Engineering Evaluation Documentation Outline to support a Qualitative Assessment	
Topical Area	Description
Step 1—Identification	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. • What are all of the UFSAR-described design functions of the upgraded/modified components within the context of the plant system, subsystem, etc.? • Describe what design function(s) that were provided by the previously installed equipment are affected and how those same design functions will be accomplished by the modified design. Also describe any new design functions to be performed by the modified design that were not part of the original design. • What assumptions and conditions are expected for each associated design function for either safety-related or power generation purposes? 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 vulnerabilities: failure modes and undesirable behavior	Consider the possibility that the proposed modification may have introduced potential single failures and plausible common cause failures. • What are potential new undesirable behaviors of the modified system? A key consideration is that undesirable behaviors may not necessarily constitute a SSC failure, but a mis-operation. (e.g., spurious actuation) • Consider errors or failures as a result of hardware, software including operating systems, application software, combining of functions onto the same controller(s), introduction of shared resources, or common hardware and software, etc. • Are there interconnections or interdependencies among the modified SSC and other SSCs? This could be facilitated by use of digital communications, modification of control logic, common usage of hardware/software, etc. • Are there potential new sources of common cause failure being introduced that are also subject to common triggering mechanisms with those of other SSCs not being modified? • What potential failure modes or undesired behaviors may be introduced as a result of the modification (e.g. new operator interfaces, introduction of digital communications)
Step 3—Assess the effects of the identified vulnerabilities	• Could the possible new failure mode or undesired behavior lead to a plant trip or transient? • Could the possible new failure mode or undesired behavior prevent performance of a safety function of the SSC(s) being modified? • Can the possible new failure mode or undesired behavior affect the ability of other SSCs to perform their safety function? • Could the possible new failure mode of the SSC, concurrent with a similar failure of another SSC not being modified but sharing a

DRAFT FOR DISCUSSION

Table 2—Example - Engineering Evaluation Documentation Outline to support a Qualitative Assessment	
Topical Area	Description
	common vulnerability and triggering mechanism, place the plant into an unanalyzed condition, or into a condition for which the other SSC was assumed to function as expected for a particular event analyzed in the existing safety analysis? • What are the results of the postulated new failure(s) of the modified SSC(s) compared to previous evaluation results described in the UFSAR? • Does the possible new failure mode or undesired behavior affect the ability of the modified SSC or other SSCs to provide its design function (as defined in NEI 96-07)?
Step 4—Identify appropriate resolutions for each identified vulnerability	What actions are being taken (or were taken) to address significant identified vulnerabilities? • Are further actions required? • Re-design in order to add additional design features or attributes? • Credit existing backup capability? • Is there means to annunciate the postulated failure or misbehavior to the operator?
Step 5—Rationale	Provide a brief description of why the identified resolutions described in Step 4 of this table adequately address the identified vulnerabilities in Step 3 of this table.
Step 6—Documentation of Available Evidence	• An acceptable documentation describes each of the resolutions needed to address the potential low likelihood failure modes identified in Step 2 of this table • Conformance to regulatory requirements (e.g. General Design Criteria and Regulatory Guides) and Industry consensus standards, etc. that are met or credited. (e.g., seismic, EMI/RFI, ambient temperature, heat contribution, etc.), as applicable. • Quality of the Design Processes employed in such as within the software life cycle development (e.g., verification and validation processes used as evident in a traceability matrix, quality assurance (QA) documentation, unit test and system test results, etc.,), • Description of relevant Operating History (e.g., platform used in numerous applications worldwide, etc. with minimal failure history, etc.) • Description of how the design features/attributes are credited towards resolution of the vulnerabilities identified (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(s)), defense-in-depth (e.g., internal systematic diversity, internal back-up capability, etc.) • Engineering evaluations performed such as failure analysis, dependability analysis, defense-in-depth analysis, etc.

DRAFT FOR DISCUSSION

Table 2—Example - Engineering Evaluation Documentation Outline to support a Qualitative Assessment	
Topical Area	Description
Step 7—Conclusion	Apply the results of the engineering evaluation to the qualitative assessment to respond to the 50.59 evaluation questions as appropriate.

6. Qualitative Assessment Documentation

NRC 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 principals 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. Documentation of referenced documents includes the document name and location of the information within any referenced document.

If the qualitative assessment categories discussed in Section 4.3 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.

DRAFT FOR DISCUSSION

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

DRAFT FOR DISCUSSION