HILARY LANE
Director, Fuel and Radiation Safety

1201 F Street NW, Suite 1100
Washington, DC 20004
P: 202.341.7951
hml@nei.org
nei.org

NUCLEAR ENERGY INSTITUTE

April 18, 2023

Mr. Mohamed Shams
Office of Nuclear Reactor Regulation
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

Subject: Request for Review and Endorsement of NEI 23-03, "Supplemental Guidance for Application of 10 CFR 50.59 to Digital Modifications at Non-Power Production or Utilization Facilities."

Project Number: 689

Dear Mr. Shams:

The Nuclear Energy Institute (NEI)[1] is pleased to submit for NRC's review and endorsement NEI 23-03, "Supplemental Guidance for Application of 10 CFR 50.59 to Digital Modifications at Non-Power Production or Utilization Facilities." This document was developed with assistance from the National Organization of Test, Research, and Training Reactors (TRTR), and other non-power production or utilization facility (NPUF)[2] licensees.

NEI 23-03 was developed to provide guidance for the implementation of 10 CFR 50.59 digital modifications at NPUFs. For consistency, efficiency, and ease of review, it is modeled after NEI 96-07, Revision 1, "Guidelines for 10 CFR 50.59 Implementation," which was issued in 2000 and endorsed by the NRC, as well as NEI 21-06, Revision 1, which was also endorsed by the NRC in 2022.

NEI believes that there is mutual interest in reviewing and endorsing NEI 23-03. We also would like to note our appreciation for the work that was successfully completed by your staff on the companion document to NEI 23-03 (NEI 21-06, Rev. 1, "Guidelines for 10 CFR 50.59 Implementation at Non-Power Production or Utilization Facilities"). We applaud the close coordination of that project, which resulted in a "clean" endorsement of NEI 21-06, Rev. 1, via NRC Regulatory Guide (RG) 2.8, "Guidance for Implementation of 10

[1] The Nuclear Energy Institute (NEI) is responsible for establishing unified policy on behalf of its members relating to matters affecting the nuclear energy industry, including the regulatory aspects of generic operational and technical issues. NEI's members include entities licensed to operate commercial nuclear power plants in the United States, nuclear plant designers, major architect and engineering firms, fuel cycle facilities, nuclear materials licensees, and other organizations involved in the nuclear energy industry.

[2] NPUFs collectively refer to non-power reactors and certain other production or utilization facilities that are licensed under 10 CFR 50.21, "Class 104 licensees; for medical therapy and research and development facilities," paragraphs (a) and (c) or 10 CFR 50.22, "Class 103 licenses; for commercial and industrial facilities." NPUFs do not include nuclear power reactors or production facilities as defined under paragraphs (1) and (2) of the definition of "production facility" in 10 CFR 50.2, "Definitions."

CFR 50.59, "Changes, Tests and Experiments," at Non-Power Production or Utilization Facilities," issued in February 2022. We also appreciated that this work was conducted under an expedited review schedule, during the peak of the pandemic, which was most beneficial for the licensees involved in the project, and to those who are now relying upon the endorsed guidance. This dedicated project embodied the NRC's Principles of Good Regulation.

For your awareness, NEI is submitting a fee exemption request to the NRC's Office of the Chief Financial Officer (CFO) to cover all activities involved in the review and endorsement of NEI 23-03. While we encourage NRC staff to begin their review of this document, NEI does not agree to any Part 170 fees should the CFO deny NEI's fee waiver request.

On behalf of the TRTR and NPUF community, we look forward to future engagements with NRR staff, with the mutual goal of endorsing this proposed guidance, for the benefit of NRC and licensees alike.

Please contact me should you have any questions.

Sincerely,

Hilary Lane

Attachment

c: Josh Borromeo, NRR
Duane Hardesty, NRR
Jere Jenkins, Chair of TRTR
NRC Document Control Desk

SUPPLEMENTAL GUIDANCE FOR APPLICATION OF 10 CFR 50.59 TO DIGITAL MODIFICATIONS AT NON-POWER PRODUCTION OR UTILIZATION FACILITIES

Prepared by the Nuclear Energy Institute
April 2023

Revision Table

Revision	Description of Changes	Date Modified	Responsible Person

Acknowledgements

This guideline was prepared by an NPUF 50.59 Working Group formed jointly by the National Organization of Test, Research and Training Reactors (TRTR) and NEI. This is the same working group which prepared NEI 21-06, Rev 1, "Guidelines For 10 CFR 50.59 Implementation at Non-Power Production or Utilization Facilities." The TRTR membership of the working group is shown below:

Steve Reese, Chair	Oregon State University
Jeff Bartelme	SHINE Technologies, LLC
Thomas Eiden	Atomic Alchemy Inc.
Jeff Geuther	Pennsylvania State University
Michael Grochowski	Atomic Alchemy Inc.
Corey Hines	Washington State University
Jere Jenkins	Texas A&M University
John Keffer	University of California – Irvine
Scott Lassel	North Carolina State University
Thomas Newton	National Institute of Standards and Technology
Sean O'Kelly	Idaho National Laboratory
Dagistan Sahin	National Institute of Standards and Technology
Andrew Smolinski	Armed Forces Radiobiology Research Institute
Randolph Strader	National Institute of Standards and Technology
James Whipple	National Institute of Standards and Technology

The working group wishes to acknowledge the contributions of many individuals in the industry and the Nuclear Regulatory Commission, who reviewed and commented on the drafts of this guideline. The suggestions and comments they provided have been extremely helpful in developing a workable approach for licensing digital upgrades at NPUFs.

Notice

Neither NEI, nor any of its employees, members, supporting organizations, contractors, or consultants make any warranty, expressed or implied, or assume any legal responsibility for the accuracy or completeness of, or assume any liability for damages resulting from any use of, any information apparatus, methods, or process disclosed in this report or that such may not infringe privately owned rights.

Executive Summary

NEI 23-03, “Supplemental Guidance for Application of 10 CFR 50.59 to Digital Modifications at Non-Power Production or Utilization Facilities,” provides focused application of the 10 CFR 50.59 guidance contained in NEI 21-06, Rev 1, “Guidelines For 10 CFR 50.59 Implementation at Non-Power Production or Utilization Facilities,” to activities involving digital modifications.

The main objective of this guidance is to provide all stakeholders a common framework and understanding of how to apply the 10 CFR 50.59 process to activities involving digital modifications.

The guidance in this document is based largely on the 10 CFR 50.59-related guidance contained in NEI 01-01/ EPRI TR-102348 Rev 1, “Guideline on Licensing of Digital Upgrades,” and NEI 96-07 Appendix D, Rev 1, “Supplemental Guidance for applications of 10 CFR 50.59 to Digital Modifications.” It incorporates the 10 CFR 50.59-related guidance contained in Regulatory Issue Summary (RIS) 2002-22, Supplement 1, “Clarification on Endorsement of Nuclear Energy Institute Guidance in Designing Digital Upgrades in Instrumentation and Control Systems,” and Regulatory Guide 1.187, Revision 3, “Guidance for Implementation of 10 CFR 50.59, “Changes, Tests, and Experiments.”

Table of Contents

Table of Figures

Table of Tables

1 INTRODUCTION

There are specific considerations that should be addressed as part of the 10 CFR 50.59 process when performing 10 CFR 50.59 reviews for digital modifications. These specific considerations include different potential failure modes of digital equipment; as opposed to the equipment being replaced, the effect of combining functions of previously separate devices (at the component level, at the system level, or at the "multi-system" level) into fewer devices or one device, and the potential for software common cause failure (software CCF).

The format of this document was aligned with NEI 21-06, Rev. 1 text, for ease of use. As such, there will be sections where no additional guidance is provided.

1.1 Background

Licensees have a need to modify existing systems and components due to the growing problems of obsolescence, difficulty in obtaining replacement parts, and increased maintenance costs. Also, there is great incentive to take advantage of modern digital technologies that offer potential performance and reliability improvements.

In 2002, a joint effort between the Electric Power Research Institute (EPRI) and the Nuclear Energy Institute (NEI) produced NEI 01-01, Revision 0 (also known as EPRI TR-102348, Revision 1), “Guideline on Licensing Digital Upgrades: A Revision of EPRI TR-102348 to Reflect Changes to the 10 CFR 50.59 Rule,” which was endorsed (with qualifications) by the Nuclear Regulatory Commission (NRC) in Regulatory Issue Summary (RIS) 2002-22.

Since the issuance of NEI 01-01 in 2002, digital modifications have become more prevalent. Application of the 10 CFR 50.59 guidance contained in NEI 01-01 has not been consistent or thorough across the industry, leading to NRC concerns regarding uncertainty as to the effectiveness of NEI 01-01 and the need for clarity to ensure an appropriate level of rigor is being applied to a wide variety of activities involving digital modifications.

NEI 01-01 contained guidance for both the technical development and design of digital modifications, as well as the application of 10 CFR 50.59 to those digital modifications. The NRC also identified this "mixture of guidance" as an issue and stated that NEI should separate the technical guidance from the 10 CFR 50.59 guidance.

In 2018, Supplement 1 to RIS 2002-22 was issued to clarify the NRC staff’s endorsement of the guidance pertaining to NEI 01-01, Sections 4 and 5 and Appendices A and B. Specifically, the RIS supplement clarified the guidance for preparing and documenting “qualitative assessments” that may be used to evaluate the likelihood of failure of a proposed digital modification, including the likelihood of failure due to a software common cause failure.

Supplement 1 to RIS 2002-22 identified that a qualitative assessment may be used to support a conclusion that a proposed digital I&C modification will not result in more than a minimal increase in the frequency of occurrence of accidents or in the likelihood of occurrence of malfunctions (10 CFR 50.59(c)(2)(i) and (ii)). A qualitative assessment may also be used to support a conclusion that the proposed modification does not create the possibility of an accident of a different type or a malfunction

with a different result than previously evaluated in the updated final safety analysis report (10 CFR 50.59(c)(2)(v) and (vi)).

In 2022, NEI 21-06, Rev. 1, was created to provide guidance for developing effective and consistent 10 CFR 50.59 implementation processes at a "non-power production, or utilization facility" (NPUF). NPUFs include non-power reactors, research reactors, testing facilities (also referred to as test reactors), critical assemblies, and training reactors, as well as non-power production or utilization facilities that do not have a reactor (e.g., medical radioisotope irradiation and processing facilities).

The document herein should not be considered a stand-alone document, as it represents a companion to NEI 21-06, Rev. 1, providing NPUF-specific guidance on performing 10 CFR 50.59 screens and evaluations for activities that involve digital components or modifications. It is incumbent upon the reader of this document to be familiar with the concepts, definitions, and processes for meeting the requirements of 10 CFR 50.59. To the extent possible, the section headings of this document will be consistent with that found in NEI 21-06, Rev. 1, making it easier on the reader to reference where in the 10 CFR 50.59 process these digital aspects apply.

1.2 Purpose

This document is intended to assist NPUF licensees in the performance of 10 CFR 50.59 reviews of activities involving digital modifications in a consistent and comprehensive manner. This assistance includes guidance for performing 10 CFR 50.59 Screens and 10 CFR 50.59 Evaluations. This document does not alter and, unless explicitly noted, should not be interpreted differently than the guidance contained in NEI 96-07, Rev. 1 or NEI 01-01, Rev. 1.

This document provides focused guidance for the application of 10 CFR 50.59 to activities involving digital modifications at NPUFs. This document should reflect several aspects that differentiate typical NPUFs to nuclear power reactors, around which the previous guidance is designed. These differences include:

- **Applicability of 10 CFR 50, Appendix A**. This regulation does not apply to NPUFs. Guidance on design requirements is found in NUREG-1537. However, that guidance is not as explicit as the General Design Criteria found in 10 CFR 50, Appendix A. The difference reveals itself during discussion of design bases and design basis functions in previous guidance on digital modifications. This is fundamentally important as this document attempts to determine when an activity involving a digital modification does in fact change or alter a design basis or design basis function. As some design bases and design basis functions may not be explicitly called out in an NPUF UFSAR, it may fall to the user to make a reasonable and knowledgeable conclusion as to the appropriate design bases and design bases functions for a particular system, structure, or component.

- **Applicability of 10 CFR 50, Appendix B**. This regulation does not apply to NPUFs. A quality assurance plan is required for NPUFs at the construction licensing phase. A quality assurance plan is also required for the shipment of spent fuel. However, while a quality assurance plan is not required for an operational license, the requirements for quality assurance in 10 CFR 50.34(b)(6)(ii) for a research reactor for an operational license are covered by robust technical specifications and following the guidance given in NUREG-1537 and ANSI/ANS 15.1. Therefore, this document avoids the use of formal quality assurance plans as the basis for applicability.

- **Power (size) and Potential for Public Dose**. The inventory of radioactive material in NPUFs is typically many orders of magnitude lower than a nuclear power reactor. Based upon this and reflecting the robust designs, inherent conservative nature of the maximum hypothetical accident philosophy, and robust technical specifications, this document will take a risk-informed approach. Furthermore, it is understood that the staff at some NPUFs may not be very large and not have the subject matter expertise in particular areas. Examples of this include less rigorousness or formal facility modification package process or engineering evaluations at some NPUFs.

- **Applicability of Probabilistic Risk Assessment (PRA)**. Very few NPUFs have undergone a PRA due to their inherent simplicity and low risk for dose to the public. Some aspects of the 10 CFR 50.59 process allow for PRA information to be used to determine the impact of a proposed activity on the frequency of occurrence of an accident or malfunction. This document will reflect that this information is likely not available at NPUFs and that qualitative engineering judgement needs to replace quantitative determinations when necessary.

- **Applicability of Nuclear Power Plant Guidance**. The diversity of the NPUF fleet—from 5-Watt AGN reactors to large test reactors and subcritical facilities with insignificant source-terms—make the application of a one-size-fits-all approach cumbersome. Furthermore, the applicability of nuclear power plant standards and guidance to NPUFs is potentially overly burdensome, e.g., 10 CFR 50 Appendix B Quality Assurance programs are not required for manufacturers of digital systems for NPUFs.

The guidance in this document applies to 10 CFR 50.59 reviews for both small-scale and large-scale digital modifications; from the simple replacement of an individual analog meter with a microprocessor-based instrument, to a complete replacement of an analog reactor protection system with an integrated digital system. Examples of activities considered to involve a digital modification include computers, computer programs, data (and its presentation), embedded digital devices, software, firmware, hardware, the human-system interface, microprocessors, and programmable digital devices (e.g., Programmable Logic Controllers and Field Programmable Gate Arrays).

This guidance is not limited to "stand-alone" instrumentation and control systems. This guidance can also be applied to the digital aspects of modifications or replacements of mechanical or electrical equipment if the new equipment makes use of digital technology (e.g., a new HVAC design that includes embedded microprocessors for control).

Finally, this guidance is applicable to digital modifications involving safety-related and non-safety-related systems and components, and also covers “digital-to-digital” activities (i.e., modifications or replacements of digital-based systems).

1.3 10 CFR 50.59 Process Summary

As part of making a change to an NPUF, the licensee performs the necessary reviews and evaluations to ensure that the change is safe, verifies that the change meets the applicable regulations, determines the effect of the change on the plant’s licensing basis, and determines whether approval of the change is needed from the NRC. The key regulation that governs changes to a licensed nuclear facility is 10 CFR 50.59.

Under the provisions of 10 CFR 50.59, the licensee is allowed to (a) make changes to the facility as described in the Updated Final Safety Analysis Report (UFSAR), (b) make changes to the procedures as described in the UFSAR, and (c) conduct tests or experiments not described in the UFSAR, without NRC review and approval prior to implementation, provided the proposed activity does not involve a change in the Technical Specifications and meets the criteria defined in 10 CFR 50.59.

The 10 CFR 50.59 process, shown in Figure 1.1, applies to digital upgrades as it does to other facility modifications. However, there are specific considerations that should be addressed including, for example, different potential failure modes of digital equipment as opposed to the equipment being replaced, the effect of combining functions of previously separate devices into one digital device, and the potential for software common cause failures. These digital considerations are addressed in the design process, including in failure analyses and other engineering evaluations.

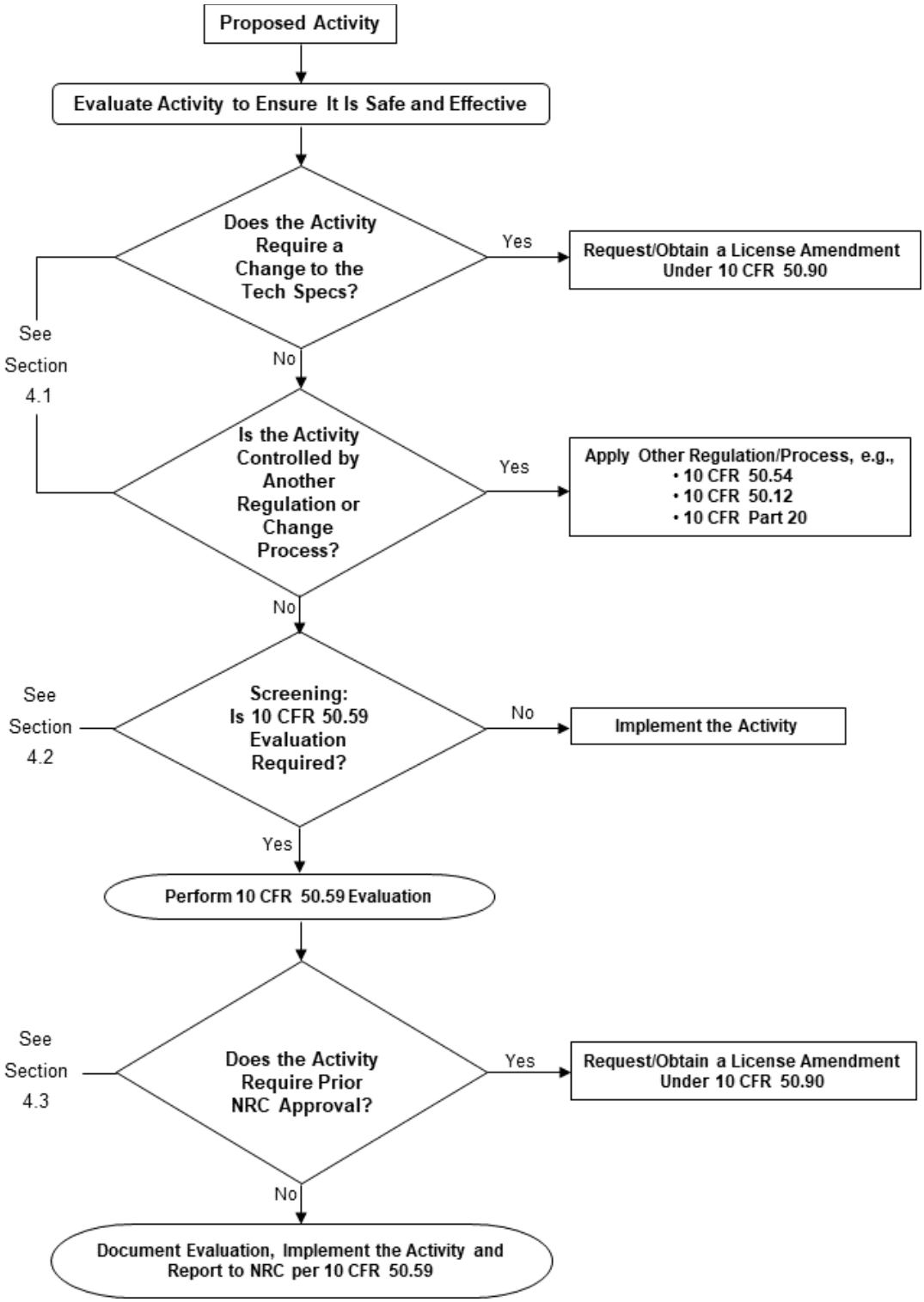

Figure 1.1: 10 CFR 50.59 Process

2 DEFENSE IN DEPTH DESIGN PHILOSOPHY AND 10 CFR 50.59

See Section 2 of NEI 21-06, Rev 1. No additional guidance is provided.

3 DEFINITIONS AND APPLICABILITY OF TERMS

Definitions 3.1 through 3.14 are the same as those provided in NEI 21-06, Rev 1. Definitions specific to this document represent a continuation of that list and are defined below.

3.15 Qualitative Assessment

Definition:

A **qualitative assessment** is a specific type of technical-based engineering evaluation useful to 10 CFR 50.59 Evaluations when responding to Evaluation criteria 10 CFR 50.59(c)(2(i), (ii), (v) and (vi).

Discussion:

The purpose of a **qualitative assessment** is to determine the failure likelihood of a digital equipment failure. The failure likelihood can be either *sufficiently low* (see the definition in Section 3.16) or *not sufficiently low*. If the qualitative assessment concludes the digital equipment failure likelihood is "sufficiently low," then by extension, the likelihood of a software CCF is also considered to be "sufficiently low." Therefore, the only part of the **qualitative assessment** needed for responding to the four 10 CFR 50.59(c)(2) criteria listed above is the outcome (i.e., *sufficiently low* or *not sufficiently low*).

Although a **qualitative assessment** could be performed as part of developing the responses to the four 10 CFR 50.59(c)(2) criteria listed above, this technical-based engineering evaluation is typically performed "prior to" or "in parallel with" the completion of the 10 CFR 50.59 Evaluation.

Generally, reasonable assurance of the low likelihood of failure due to a software CCF is derived from the **qualitative assessment** of factors involving (1) the design attributes of the modified SSC, (2) the quality of the design processes, and (3) the operating experience of the software and hardware used (i.e., product maturity and in-service experience).

The **qualitative assessment** is used to record the factors and rationale for making a determination of the likelihood of failure (i.e., *sufficiently low* or *not sufficiently low*) due to a software CCF that a digital I&C modification will exhibit.

The determination of the likelihood of failure may consider the aggregate of all the factors described above. Namely, some of the factors may compensate for weaknesses in other areas or other factors. For example, thorough testing coupled with an analysis demonstrating that untested states are accounted for in the proposed application may provide additional assurance of a *sufficiently low* likelihood of failure to compensate for a lack of operating experience.

A **qualitative assessment** should not be used for digital I&C replacements of the reactor protection system (RPS), the engineered safety features actuation system (ESFAS), or modification/replacement of the internal logic portions of these systems (e.g., voting logic, bistable inputs, and signal conditioning/processing).

A **qualitative assessment** should not be used in the 10 CFR 50.59 screening process when determining if a change is adverse to a design function. As described in NRC RIS 2002-22 Supplement 1, a qualitative assessment can be used to support a conclusion that a proposed digital I&C modification will not result in more than a minimal increase in the frequency of occurrence of accidents or in the likelihood of occurrence of malfunctions. A qualitative assessment can also be used to support a conclusion that the proposed modification does not create the possibility of an accident of a different type or malfunction with a different result than previously evaluated in the updated final safety analysis report.

3.16 Sufficiently Low

Definition:

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 errors and calibration errors).

Discussion:

This **sufficiently low** threshold is not interchangeable with that used for distinguishing between events that are “credible” or “not credible.” The threshold for determining if an event is credible uses the criterion of “as likely as” (i.e., not “much lower than”) the malfunctions already assumed in the UFSAR.

3.17 Common Cause Failures

Definition:

A common cause failure is the failure of equipment or systems that occur as a consequence of the same cause.

Discussion:

The term is usually used with reference to redundant equipment or systems or to uses of identical equipment in multiple systems. Common cause failures can occur due to design, operational, environmental, or human factor initiators. Common cause failures in redundant systems compromise safety if the failures are concurrent failures, that is, failures which occur over a time interval during which it is not plausible that the failures would be corrected. Common mode failure, by strict interpretation, has a meaning that is somewhat different from common cause failure because failure mode refers to the manner in which a component fails rather than the cause of the failure. However, because the discussions in this guideline are concerned with failures that can compromise safety and disable redundant systems or disable multiple systems using the same equipment, regardless of whether they are common mode or common cause, the two terms are used interchangeably in this document. [Definitions adapted from the EPRI Equipment Qualification Reference Manual TR-100516 and ANSI/IEEE 352-1987]

3.18 Consequences

Definition:

In 10 CFR 50.59, the term “consequences” refers to radiological doses, to either the public or workers, as a result of any accident evaluated in the UFSAR.

Discussion:

This does not apply to the occupational exposures resulting from routine operations, maintenance, testing, etc.

3.19 Digital Upgrade

Definition:

A digital upgrade is a modification to a plant system or component which involves installation of equipment containing one or more programmable digital devices.

Discussion:

These upgrades are often made to plant instrumentation and control (I&C) systems, but the term as used in this document also applies to the replacement of mechanical or electrical equipment when the new equipment contains a computer (e.g., installation of a new heating and ventilation system which includes controls that use one or more embedded microprocessors), as well as software changes to an existing digital system. Programmable digital devices include technologies such as field programmable gate arrays, computers, or programable logic controllers. A computer, used broadly in this document, is used to refer to any device which includes digital computer hardware, software (including firmware), and interfaces. A microprocessor is considered as one type of computer. [Derived from IEEE 7-4.3.2-1993]

3.20 Diversity

Definition:

The use of at least two different means for performing the same function.

Discussion:

Diversity can include how the function is performed (e.g., different algorithms, different variables sensed or physical principles applied, manual versus automatic) or in the equipment (different technologies, different hardware and/or software, different actuation means) used to perform the function. [Derived from IEC 880, the EPRI Equipment Qualification Reference Manual TR-100516, NUREG/CR-6303, and NUREG 800 Branch Technical Position (BTP)/HICB-19]

3.21 Human-system interface (HSI)

Definition:

Human-system Interfaces include all interfaces between the digital system and plant personnel including operators, maintenance technicians, and engineering personnel.

Discussion:

These interfaces include information and control resources used by plant personnel to perform their duties and tasks. Currently HSI is the term that is synonymous with and replacing human-machine interface (HMI) and man-machine interface (MMI). Principal HSIs are: alarms, information displays (including procedures), and controls. An HSI may be made up of hardware and software components and is characterized in terms of its important physical and functional characteristics. Examples include display or control interfaces, test panels, and configuration terminals.

3.22 Redundancy

Definition:

The provision of alternative (identical or diverse) equipment or systems so that any one can perform the required function, regardless of the state of operation or failure of any other. [Derived from IEC 880]

Discussion:

Redundancy implies a need to have more than one system capable of performing the intended function and is not limited to safety related systems, structures, and components. This is usually utilized in systems where defense in depth is required to design against the single failure criterion.

3.23 Safety related systems, structures, and components (SSCs)

Definition:

Those systems, structures, and components that are relied upon to remain functional during and following design basis events to ensure (1) the integrity of the reactor coolant pressure boundary, (2) the capability to shut down the reactor and maintain it in a safe shutdown condition, or (3) the capability to prevent or mitigate the consequences of accidents that could result in potential offsite exposures comparable to the applicable guideline exposures set forth in section 50.34 (a)(1) or section 100.11 of 10 CFR. [10 CFR 50.2]

Discussion:

Only the first two parts of this apply to NPUFs. Part 3 only applies to test reactors.

3.24 Software

Definition:

Computer programs, procedures, and possibly associated documentation and data pertaining to the operation of a computer system. [derived from ANSI/IEEE 610.12-1990]

Discussion:

Software is a set of instructions, data or programs used to operate computers and execute specific tasks. Software is a generic term used to refer to applications, scripts and programs that run on a device. This includes software that is implemented as firmware and operating systems.

3.25 Software safety analysis

Definition:

The process of identifying and analyzing potential hazards (which may result either from failures of the digital system or from external conditions or events) that can affect the safety of the system and the facility.

Discussion:

The process focuses on identifying requirements that are needed in order to prevent or mitigate hazards. Regulatory review guidance in BTP/HICB-14 and in Regulatory Guide 1.173 states that there should be a defined safety analysis process in which responsibilities and activities are defined for each phase of the development process.

3.26 System-level failure

Definition:

The failure of a system to perform its function, or a failure which affects the ability of another system to function.

Discussion:

This phrase is enveloped by the broader phrase “results of a malfunction of an SSC,” which refers to the effect of the malfunction of an SSC in the Safety Analysis, as discussed in NEI 21-06, Revision 1. System-level failures are usually preceded by a failure of a single component independently or from a common cause failure.

3.27 Verification and validation (V&V)

Definition:

The process of determining whether the requirements for a system or component are complete and correct, the products of each development phase fulfill the requirements or conditions imposed by the

previous phase, and the final system or component complies with specified requirements. [derived from ANSI/IEEE 610.12-1990]

Discussion:

Verification is the process to ensure that software does what it is required to do. This is typically performed by using the software to calculate benchmark problems. Validation is the process to determine if the results are accurate. Validation involves examining if the software produces results for the given conditions being analyzed.

4 IMPLEMENTATION GUIDANCE

4.1 Applicability

See Section 4.1 of NEI 21-06, Rev 1. No additional guidance is provided.

4.2 Screening

In accordance with 10 CFR 50.59, plant changes are reviewed by the licensee to determine whether the change can be made without obtaining a license amendment (i.e., without prior NRC review and approval of the change). The 10 CFR 50.59 process of determining when prior NRC review is required includes two parts: screening and evaluation. The screening process involves determining whether a change has an adverse effect on a design function described in the UFSAR; the evaluation process involves determining whether the change has more than a minimal effect on the likelihood of failure or on the consequences associated with the proposed activity.

The mere fact that a change converts analog equipment or signals to digital does not cause the change to screen in. There are other specific aspects of the change that must be considered in screening which are discussed in this section.

Figure 4.1 provides an overview of the thought process involved in 10 CFR 50.59 screening. The first step in screening is to determine whether the change affects a design function as described in the UFSAR. If it does not, then the change screens out, and can be implemented without further evaluation under the 10 CFR 50.59 process. If the change does affect a UFSAR-described design function, then it must be evaluated to determine if it has an adverse effect. Changes with adverse effects are those that have the potential to increase the likelihood of malfunctions, increase consequences, create new accidents, or otherwise meet the 10 CFR 50.59 evaluation criteria. Additional guidance on the definition of adverse is provided in the bulleted examples in Section 4.2.1 of NEI 21-06, Revision 1. These include:

- Decreasing the reliability of a design function,
- Adding or deleting an automatic or manual design function,
- Converting a feature that was automatic to manual or vice versa,
- Reducing redundancy, diversity, or defense-in-depth, or
- Adversely affecting the response time required to perform required actions.

If a change is adverse, then a 10 CFR 50.59 evaluation is performed to determine whether the specific criteria provided in 10 CFR 50.59(c)(2) are satisfied.

As stated in NEI 21-06, Rev. 01, Section 4.2.1, the determination of the impact of a proposed activity (i.e., *adverse* or *not adverse*) is based on the impact of the proposed activity on UFSAR-described design functions. To assist in determining the impact of a digital modification on a UFSAR-described design function, the general guidance from NEI 21-06, Rev. 01 will be supplemented with the digital-specific guidance in the topic areas identified below.

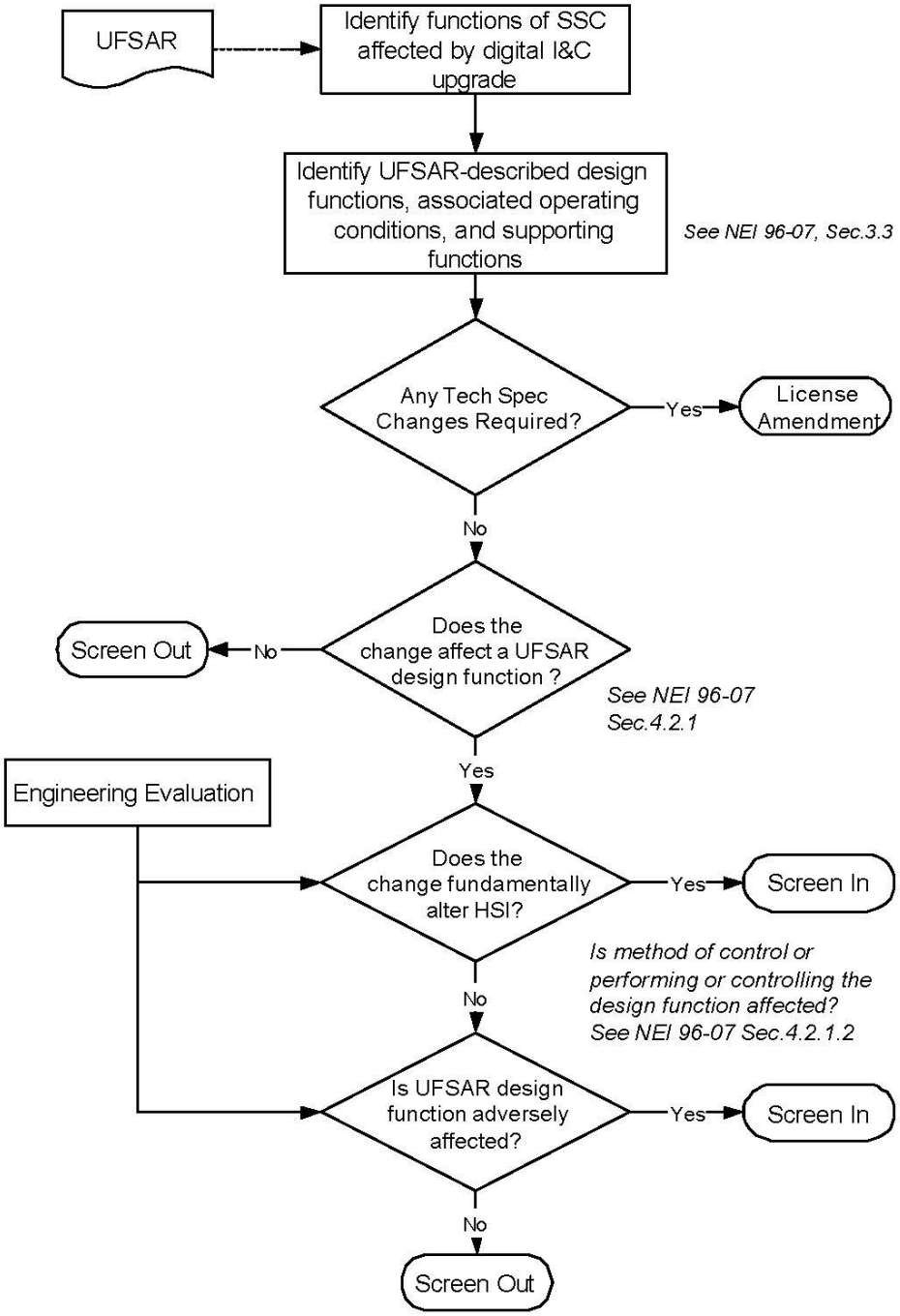

Figure 4.1: The 10 CFR 50.59 Screening Process

4.2.1 Digital-to-Digital Replacements and "Equivalency"

In NEI 21-06, Rev. 01, Section 4.2.1.1, equivalent replacements are discussed. However, digital-to-digital changes may not necessarily be equivalent because the component/system behaviors, response times,

failure modes, etc. for the new component/system may be different from the old component/system. All non-equivalent digital-to-digital replacements should utilize the guidance provided in this document.

4.2.2 Is the Activity a Change to the Facility or Procedures as Described in the UFSAR?

There is no regulatory requirement for a proposed activity involving a digital modification to default (i.e., be mandatorily "forced") to an adverse conclusion.

Although there may be adverse impacts on UFSAR-described design functions due to the following types of activities involving a digital modification, these typical activities do not default to an adverse conclusion simply because of the activities themselves.

- The introduction of software or digital devices.
- The replacement of software and/or digital devices with other software and/or digital devices.
- The use of a digital processor to "calculate" a numerical value or "generate" a control signal using software in place of using analog components.
- Replacement of hard controls (e.g., pushbuttons, knobs, switches, etc.) with a touch-screen to operate or control plant equipment.

Engineering/technical information should be documented (as part of the design process) to record the impacts from digital modifications. This engineering/technical information will be used as the basis/justification for the conclusion of *adverse* or *not adverse*.

4.2.2.1 Scope of Digital Modifications

Generally, a digital modification may consist of three areas of activities:

1. software-related activities,
2. hardware-related activities, or;
3. Human-System Interface-related activities.

NEI 21-06, Rev. 01, Section 4.2.1.1, provides guidance for activities that involve "...an SSC design function..." or a "...method of performing or controlling a design function..." and Section 4.2.1.2 provides guidance for activities that involve "...how SSC design functions are performed or controlled (including changes to UFSAR-described procedures, assumed operator actions and response times)."

Based on this segmentation of activities, the software and hardware portions will be assessed within the "facility" screen consideration since these aspects involve SSCs, SSC design functions, or the method of performing or controlling a design function and the Human-System Interface portion will be assessed within the "procedures" screen consideration since this portion involves how SSCs are operated and controlled.

4.2.2.2 When Are Digital Modifications Adverse?

What does “adverse” mean? The first step in screening is to determine whether the change affects a design function as described in the UFSAR. If it does not, the change screens out, and can be implemented without further evaluation under the 10 CFR 50.59 process. If the change does affect a UFSAR-described design function, then it must be evaluated to determine if it has an adverse effect. Changes with adverse effects are those that have the potential to increase the likelihood of malfunctions, increase consequences, create new accidents, or otherwise meet the 10 CFR 50.59 evaluation criteria. Additional guidance on the definition of adverse is provided in the bulleted examples in Section 4.2.1 of NEI 21-06, Revision 1. These include:

- Decreasing the reliability of a design function,
- Adding or deleting an automatic or manual design function,
- Converting a feature that was automatic to manual or vice versa,
- Reducing redundancy, diversity, or defense-in-depth, or
- Adversely affecting the response time required to perform required actions.

If a change is adverse, then a 10 CFR 50.59 evaluation is performed to determine whether the specific criteria provided in 10 CFR 50.59(c)(2) are satisfied.

With respect to screening digital upgrades, one important question is whether adverse effects are created by software. An adverse effect may be the potential marginal increase in likelihood of failure due to the introduction of software. For redundant safety systems, this marginal increase in likelihood creates a similar marginal increase in the likelihood of a common failure in redundant channels. On this basis, most digital upgrades to redundant safety systems should be conservatively treated as “adverse” and screened in for further evaluation under the 10 CFR 50.59 process.

However, for some relatively simple digital equipment, engineering evaluations may show that the risk of failure due to software is not significant and need not be evaluated further, even in applications of high safety significance. As described in Section 4.3.1.1 of NEI 21-06, Rev 1, consensus methods have been developed for evaluating dependability of digital equipment including assessment of the potential for common cause failure due to software. Overall, the ability to evaluate the dependability of digital equipment has improved over the years, as some vendors are using updated and improved processes for software and digital system development, V&V and configuration management. Also, some digital equipment has gained extensive operating history, both inside and outside the nuclear industry.

Thus, for some upgrades the likelihood of failure due to software may be judged to be no greater than failure due to other causes, i.e., comparable to hardware common cause failure. In such a case, even when it affects redundant systems, the digital upgrade would screen out.

In addition to the software question, other characteristics of a digital upgrade could cause the change to screen in to a 10 CFR 50.59 evaluation. Some potentially adverse effects that should be considered when screening digital upgrades include:

- Combining previously separate functions into one digital device such that failures create new malfunctions (e.g., multiple functions are disabled if the digital device fails).
- Changing performance from UFSAR-described requirements (e.g., for response time, accuracy, etc.).
- Changing functionality in a way that increases complexity, potentially creating new malfunctions.
- Introducing different behavior or potential failure modes (for which the risk is not negligible) that could affect the design function.

4.2.2.3 Screening of Changes to the Facility as Described in the UFSAR

In the determination of potential adverse impacts, the following aspects should be addressed in the response to this Screen consideration:

- Use of Software and Digital Devices
- Combination of Components/Systems and/or Functions

For applications involving SSCs with design functions, an adverse effect may be created due to the potential marginal increase in the likelihood of SSC failure due to the introduction of software. This does not mean that all digital modifications that introduce software will be considered adverse and automatically screen-in.

For redundant safety systems, this marginal increase in likelihood creates a similar marginal increase in the likelihood of a common failure in the redundant safety systems. On this basis, most digital modifications to redundant safety systems are adverse.

However, for some digital modifications, the engineering/technical information supporting the change may show that the digital modification contains design attributes to eliminate consideration of a software common cause failure. In such cases, even when a digital modification involves redundant systems, the digital modification would not be adverse.

Here the concept of “relatively simple” for an NPUF is introduced. It should be noted that this definition will differ from that provided in NEI 96-07, Appendix D. This difference is reflective of a risk informed approach towards implementing changes at NPUFs as compared to power reactors. Relatively simple at an NPUF means a digital modification or component that can be comprehensively tested, may have a programable software or digital architecture that is reasonably understood, has limited functionality, and was obtained from a reputable commercial manufacturer.

To reach a screen conclusion of *not adverse* for relatively simple digital modifications, the degree of assurance needed to make that conclusion is based on considerations of the *physical characteristics* of the digital modification. Example considerations include:

- Is the change limited in scope (e.g., replacing a single analog component with a single digital component)?
- Uses a relatively simple digital architecture internally (e.g., simple process of acquiring an input signal(s), setting an output signal(s), and performing some simple diagnostic checks.)
- Does it have limited functionality (e.g., how many signal inputs and outputs are there and how the output signals are being used).
- Can it be comprehensively tested (but not necessarily 100 percent of all combinations)
- For field programable components or PLCs, can access to software/hardware programing be controlled?
- For field programable components or PLCs, is the programing logic easily understood?
- Was the component manufactured from a reputable manufacturer under a quality assurance program with a demonstrable history of use?

For relatively simple digital modifications, engineering/technical information supporting the change may be used to show that the digital modification would not adversely affect design functions; even for digital modifications that involve redundant components/systems, because a software CCF is not introduced.

Additionally, to reach a screen conclusion of *not adverse* for relatively simple digital modifications, the degree of assurance needed to make that conclusion is based on considerations of the *engineering evaluation assessments* including:

- The quality of the design processes employed
- Single failures of the digital device are encompassed by existing failures of the analog device (e.g., no new digital communications among devices that introduce possible new failure modes involving separate devices)
- Has extensive applicable operating history

The use of different software in two or more channels, trains or loops of SSCs is *not adverse* due to a software CCF because there is no mechanism to create a new malfunction due to the introduction of the software.

Some specific examples of activities that have the potential to cause an *adverse* effect include the following activities:

- Addition or removal of a dead-band, or

- Replacement of instantaneous readings with time-averaged readings (or vice-versa).

In each of these specific examples, the impact on a design function associated with the stated condition needs to be assessed to determine the screen conclusion (i.e., *adverse* or *not adverse*).

Example 4-1. Screening for a Smart Transmitter (Screens out)

Proposed Activity Description

Transmitters are used to drive signals for parameters monitored by a ventilation control system. The original analog transmitters are to be replaced with microprocessor-based transmitters. The change is of limited scope since the existing 4-20 mA instrument loop is maintained for each channel without any changes other than replacing the transmitter itself. The digital transmitters are used to drive signals of monitored parameters and thus have limited functionality with respect to the ventilation system design function. The design function of the ventilation system is to provide removal of airborne radioactive materials through a controlled path and to shut down upon detection of high levels of airborne radioactive materials. The ventilation system is not considered an engineered safety feature.

The digital transmitters use a relatively simple digital architecture internally and can be thoroughly tested. Failures of the new digital device are encompassed by the failures of the existing analog device. The engineering/technical information supporting the change concluded that the digital system is at least as reliable as the previous system, the conclusion of which is based on the quality of the design processes employed, and the operating history of the software and hardware used. In addition, based on the simplicity of the device (minimal input/output), it was comprehensively tested. Further, substantial operating history has demonstrated high reliability in applications similar to the ventilation system application.

Screen Response

The proposed digital modification is *not adverse* (for the aspect being illustrated in this example) because the digital modification is relatively simple and the assessment of the considerations identified above has determined that the reliability of performing the design function is not reduced and a software CCF is not introduced.

Example 4-2. Screening for a Smart Transmitter (Screens in)

Proposed Activity Description

Transmitters are used to drive signals for parameters monitored by a ventilation control system. The original analog transmitters are to be replaced with microprocessor-based transmitters. The digital transmitters are used to drive signals of monitored parameters and thus have limited functionality with respect to the ventilation system design function. The design function of the ventilation system is to provide removal of airborne radioactive materials through a controlled path and to shut down upon detection of high levels of airborne radioactive materials. The ventilation system is not considered an engineered safety feature. The new transmitters have the capability to transmit their output signal using a digital communication protocol. Other instruments in the loop are to be replaced with units that can communicate with the transmitter using the same protocol.

The digital transmitters use a relatively simple digital architecture internally and can be thoroughly tested. Failures of the new digital device are encompassed by the failures of the existing analog device. The engineering/technical information supporting the change concluded that the digital system is at least as reliable as the previous system, the conclusion of which is based on the quality of the design processes employed, and the operating history of the software and hardware used. In addition, based on the simplicity of the device (minimal input/output), it was comprehensively tested. Further, substantial operating history has demonstrated high reliability in applications similar to the ventilation system application.

Screen Response

The proposed digital modification is *adverse* (for the aspect being illustrated in this example) because this change not only upgrades to a digital transmitter, but also converts the instrument loop to digital communications among devices (fundamentally alters the existing means of performing the design function). There would be the potential for adverse effects owing to the digital communication and possible new failure modes involving multiple devices (a potential software CCF). As a result, this change screens in.

Example 4-3. Screening for a Recorder Upgrade (Screens out)

Proposed Activity Description

An analog recorder is to be replaced with a new microprocessor-based recorder. The recorder is used to display data on the airborne radioactive material monitoring system within the reactor bay. The analog recorder is a simple ink strip chart showing a waterfall display. An engineering/technical evaluation performed on the change determined that the new recorder will be highly dependable (based on a quality development process, testability, and successful operating history) and therefore, the risk of failure of the recorder due to software is considered sufficiently low. The new recorder also meets all current required performance, HSI, and qualification requirements, and would introduce no new failure modes or effects at the level of the design function. The operator will use the new recorder in the same way the old one was used (the digital system will also produce the same waterfall display), and the same information is provided.

The USFAR-described design function of the airborne radioactive material monitoring system is to measure the amount of particulate and gaseous radioactive material in the reactor bay air, alarm on a high-level condition, and initiate a shutdown of the ventilation system upon a high-level condition.

Screen Response

The activity is *not adverse* (for the aspect being illustrated in this example) on the design function of the airborne radioactive material monitoring system because the new recorder is as reliable as the existing, no new failure modes were introduced, and the method of controlling or performing the design function is unaltered. The licensee concludes that the change will not adversely affect any design function and screens out the change.

Example 4-4. Screening for a Pump Controller Upgrade (Screens In)

Proposed Activity Description

Two non-safety-related pumps are used for a cooling system of a 1-MW research reactor. One pump is used for the primary coolant system and the other is used for the secondary cooling system. There are two analog control systems (one per pump) that are physically and functionally the same.

The two analog control systems will be replaced with two PLC digital control systems. The hardware platform for each digital control system is from the same supplier and the software in each digital control system is exactly the same. No combination of components/systems and/or functions occurs as part of this digital modification. Additionally, in order to facilitate future modifications, the PLC chosen has 20 inputs and 30 outputs with a wide variety of commonly used variables within interconnecting logic.

The design function of the pumps is to control and regulate cooling water flow to both the primary and secondary sides. However, due to the water inventory present and the low power of the reactor, failure of these systems would not result in an unacceptable dose to the public.

Screen Response

There is an *adverse* impact (for the aspect being illustrated in this example) on the design function of the primary and secondary cooling system because the use of the exact same software in both digital control systems creates a potential software CCF that did not previously exist. Additionally, the digital modification associated with this proposed activity is not relatively simple, so the process for assessing relatively simple digital modifications could not be used.

Example 4-5. Screening for Software Change (Screens out)

Proposed Activity Description

A digital control system produces the primary displays used by the operator to adhere to license power limits. It is desired that the numerical display shows an additional digit of resolution and be a larger font to improve visibility. The software changes are relatively simple to make to two specific files.

The software change quality control process controlled the requirements, specific changes, and test plan, and demonstrated that the affected changes could be thoroughly tested. Therefore, the risk of failure of the primary power displays due to the software change is considered very low. The new display layout meets all current required performance, HSI, and qualification requirements, and would have no new failure modes or effects at the level of the design function. The operator will use the display in the same way the old one was used, and the same information is provided.

Screen Response

The activity is *not adverse* (for the aspect being illustrated in this example) on the design function of the power monitoring system because the method of controlling or performing the design function is

unaltered, the change is limited in scope, and can be comprehensively tested. The licensee concludes that the change will not adversely affect any design function and screens out the change.

Example 4-6. Screening for Software Change (Screens In)

Proposed Activity Description

A digital control system produces the control voltages for rod control systems used by the operator to control the reactor. The maximum reactivity addition rate is credited in the safety analysis as an assumption when calculating peak power during a transient that ensures fuel safety limits are not exceeded. It is desired that the control voltage algorithm for automatic operation be adjusted to improve performance, slowing down the rod speed to minimize power overshoot during power maneuvers. The software changes are made to several rod control files that affect rod speeds, but the same files also control indications, accuracies, and credited interlocks.

The software change quality control process controlled the requirements, specific changes, test plan and demonstrated that the affected changes could be thoroughly tested. However, an engineering evaluation determined the risk of failure of rod speed and other parts of the affected files could not be considered very low due to the complexity of the change and the potential for programming errors.

Screen Response

The activity is *adverse* (for the aspect being illustrated in this example) on the design function of controlling rod speed (reactivity addition rate) and credited interlocks. While the rod speeds are adjusted to be slower, which is not adverse, the change is not limited in scope, and the digital modification associated with this proposed activity is not relatively simple, so the process for assessing relatively simple digital modifications could not be used. The licensee concludes that the change has the potential to adversely affect design functions and screens in the change for further evaluation.

4.2.2.4 Combination of Components/Systems and/or Functions

The UFSAR may identify the number of components/systems, how the components/systems are arranged and/or how functions are allocated to those components/systems.

When replacing analog SSCs with digital SSCs, it is potentially advantageous to combine multiple components/systems and/or functions into a single device or control system. However, as a result of this combination, the failure of the single device or control system has the potential to adversely affect *design functions*.

The mere act of combining previously separate components/systems and/or functions does not make the Screen conclusion adverse. However, if combining the previously separate components/systems and/or functions causes an adverse impact on a *design function* (e.g., by causing the loss of multiple design functions when the digital device fails), then the combination aspect of the digital modification will have an adverse impact on a *design function* (i.e., screen in).

When comparing the existing and proposed configurations, consider how the proposed configuration affects the number and/or arrangement of components/systems and the potential impacts of the proposed arrangement on *design functions*.

Furthermore, digital modifications that involve networking; combining design functions from different systems; interconnectivity across channels, systems, and divisions; or shared resources, merit careful review to determine if such modifications cause reductions in the redundancy, diversity, separation, or independence of UFSAR-described design functions.

Combining different functions due to digital modifications can result in combining design functions of different systems; either directly in the same digital device, or indirectly through shared resources.

Shared resources (e.g., bidirectional communications, power supplies, controllers, and multifunction display and control stations) introduced by digital modifications may reduce the redundancy, diversity, separation, or independence of UFSAR-described design functions.

Reductions in the redundancy, diversity, separation, or independence of a UFSAR-described design function have an adverse impact on that design function.

Example 4-6. Screening for Pump Controller Upgrade (Screens Out)

Proposed Activity Description

Two non-safety-related pumps are used for a cooling system of a 1-MW research reactor. One pump is used for the primary coolant system and the other is used for the secondary cooling system. There are two analog control systems (one per pump) that are physically and functionally the same.

The two analog control systems will be replaced with two PLC digital control systems. The hardware platform for each digital control system is from different suppliers and the software in each digital control system is similar in application but functionally different. For each pump control systems, all of the analog subcomponents will be replaced with a single digital device that consolidates all of the components, sub-components and the functions associated with each component and sub-component (one digital control device for the primary and one digital control device for the secondary for a total of two devices). The components and sub-components in each analog control system will be replaced with their own digital control system, retaining two discreet, unconnected control systems. No combination of components/systems and/or functions occurs as part of this digital modification between each pump but does occur for each control system individually. However, no design functions are being combined. The PLCs have only three inputs and three outputs, the programing functions are very simple and minimal in nature, the operator cannot alter the display, and the software can be password protected. A qualitative engineering evaluation supporting this change identifies that the likelihood of failure of the software and hardware is sufficiently low.

The design function of the primary pump is to move coolant in order to remove heat from the fuel elements. The design function of the secondary pump is to move coolant in order to remove heat from the primary coolant loop. However, due to the water inventory present and the low power of the reactor, these systems are not considered safety-related systems.

Screen Response

There is *no adverse* impact (for the aspect being illustrated in this example) on the design function of the cooling water systems to automatically control and regulate cooling water due to the combination of components in each of the two channels because these digital components:

- will be independent and diverse (two independent manufacturers), and;
- the simple software architecture of the PLC and the low number of inputs and outputs is easily verifiable.

Example 4-7. Screening for a Temperature Controller Upgrade (Screens Out)

Proposed Activity Description

A temperature monitor/controller in a room containing an emergency room ventilation cooler provides an input to an air damper controller. If temperature gets too high, the temperature controller sends a signal to the air damper to open (if closed) to a predetermined initial position or, if already open, adjusts the position of the damper to allow increased air flow into the room.

Both analog controllers will be replaced with a single digital device that will perform in accordance with the original design requirements providing both temperature monitoring/control and air damper control. The programing functions of the new digital controllers are very simple and minimal in nature, the operator cannot alter the display (non-configurable), they are easily tested, and the software can be password protected. A qualitative engineering evaluation (not a qualitative assessment) supporting this change identifies that the likelihood of failure of the controller is sufficiently low.

The temperature monitor/controller performs a design function to control the temperature in the room by continuously monitoring the temperature in the room to ensure that instrumentation in the control room is maintained to prevent room temperatures to exceed manufacture recommendation on excess temperatures for some instrumentation in the reactor console. There is no lower limit on the acceptable temperature in the room.

Screen Response

In the current design, a failure of the temperature monitor/controller or the air damper controller causes the loss of the ability to control the temperature in the room. In the proposed design, the failure of the digital device causes multiple failures, but still only the loss of the ability to control the temperature in the room. With the loss of ability to control temperature in the room being the same in the current design and in the proposed design, there is no adverse impact (for the aspect being illustrated in this example) on the design function.

The combining of components/systems and/or functions that were previously completely physically and/or electrically discrete (i.e., not “coupled”) are of particular interest when determining the impact on *design functions*.

Example 4-8. Screening for a Combined Pump Controller Upgrade (Screens In)

Proposed Activity Description

Two non-safety-related pumps are used for a cooling system of a 1-MW research reactor. One pump is used for the primary coolant system and the other is used for the secondary cooling system. There are two analog control systems (one per pump) that are physically and functionally the same.

The two analog control systems will be replaced with a single PLC digital control system. All of the analog subcomponents will be replaced with a single digital device that consolidates all of the components, sub-components and the functions associated with each component and sub-component. The PLC has only three inputs and three outputs, the programing functions are very simple and minimal in nature, the operator cannot alter the display (non-configurable), it is easily tested, and the software can be password protected. A qualitative engineering evaluation supporting this change identifies that the likelihood of failure of the software and hardware is sufficiently low.

The design function of the primary pump is to move coolant in order to remove heat from the fuel elements. The design function of the secondary pump is to move coolant in order to remove heat from the primary coolant loop. However, due to the water inventory present and the low power of the reactor, these systems are not considered safety-related systems.

Screen Response

Because the failure of the new, single digital device will cause the loss of multiple design functions, the digital modification has an *adverse* impact (for the aspect being illustrated in this example) on the design functions of the primary and secondary coolant pumps.

4.2.2.5 Screening of Changes to Procedures as Described in the UFSAR and HSI

If the digital modification does not include or affect an HSI element (e.g., the replacement of a stand-alone analog relay with a digital relay that has no features involving personnel interaction and does not feed signals into any other analog or digital device), then this section does not apply and may be excluded from the screen assessment.

In NEI 21-06, Rev. 1, Section 3.11 defines procedures as follows:

> *"Procedures include UFSAR descriptions of how actions related to system operation are to be performed and controls over the performance of design functions. This includes UFSAR descriptions of operator action sequencing or response times, certain descriptions...of SSC operation and operating modes, operational...controls, and similar information."*

Although UFSARs do not typically describe the details of a specific HSI, UFSARs may describe design functions associated with the HSI.

Because the HSI involves system/component operation, this portion of a digital modification is assessed in this screen consideration. The focus of the screen assessment is on potential adverse effects due to modifications of the interface between the human user and the technical device. Note that the "human user" could involve Control Room Operators, other plant operators, maintenance personnel, engineering personnel, technicians, etc.

In the discussion of the screening process regarding performing or controlling design functions, NEI 21-06, Revision 1, Section 4.2.1.2, states that:

> *"For purposes of 10 CFR 50.59 screening, changes that fundamentally alter (replace) the existing means of performing or controlling design functions should be conservatively treated as adverse and screened in. Such changes include replacement of automatic action by manual action (or vice versa), changes to the man-machine interface, changing a valve from "locked closed" to "administratively closed" and similar changes."*

It is important to note that not all changes to the HSI fundamentally alter the means of performing or controlling design functions. Some HSI changes that accompany digital upgrades leave the method of performing functions essentially unchanged. Technical evaluations should determine whether changes to the HSI create adverse effects on design functions (including adverse effects on the licensing basis and safety analyses). Characteristics of HSI changes that could lead to potential adverse effects may include, but are not limited to:

- Changes to parameters monitored, decisions made, and actions taken in the control of plant equipment and systems during transients,
- Changes that could affect the overall response time of the human/machine system (e.g., changes that increase operator burden),
- Changes from manual to automatic initiation (or vice versa) of functions,
- Fundamental changes in data presentation (such as replacing an edgewise analog meter with a numeric display or a multipurpose CRT where access to the data requires operator interactions to display), or
- Changes that create new potential failure modes in the interaction of operators with the system (e.g., new interrelationships or interdependencies of operator actions and plant response or new ways the operator assimilates plant status information).

If the HSI changes do not exhibit these characteristics, then it may be reasonable to conclude that the "method of performing or controlling" the design function is not adversely affected. Note, however, that these characteristics focus on potential adverse effects due to changes in the physical operator interface, not procedure changes. Changes in procedures that may be required in order to implement HSI changes also need to be screened.

With respect to creation of new potential failure modes, changes to the HSI should be treated in a manner similar to software and digital equipment. Specifically, a disciplined development process in which human factors issues are considered by qualified personnel (e.g., a senior reactor operator) and evaluated using human factors verification and validation techniques should be credited for minimizing the likelihood of human errors and inadvertently introducing a new behavior or problem that did not previously exist for the old device.

As an example, if replacement of an analog control system with a digital control system introduces additional automation that alters the required operator response to a transient (for example, a valve automatically shuts as opposed to being shut by operator action), then the "method of performing or controlling" the safety function is changed and a 10 CFR 50.59 evaluation is required.

On the other hand, replacement of a strip chart recorder with a digital, paperless recorder might screen out so long as the data presentation is similar, the recorder location is unchanged, the data displayed is at least as legible as the strip chart recorder was, and the operator uses the recorder in the same way to perform the design function. Therefore, there is no fundamental change in the method of performing or controlling the design function. (This was the conclusion reached earlier in Example 4-3.)

4.2.2.6 Human Factors Engineering Evaluations

Similar to other technical evaluations, a human factors engineering (HFE) evaluation determines the impacts and outcomes of the change (e.g., personnel acts or omissions, as well as their likelihoods and effects). The licensing-based reviews (Screens and Evaluations) performed in accordance with 10 CFR 50.59 compare the impacts and new outcomes (i.e., post-modification) to the initial conditions and current outcomes (i.e., pre-modification) in order to determine the effect on design functions (in the Screen phase) and the need for a license amendment request (in the Evaluation phase).

For NPUFs, guidance on performing an HFE is provided below. For NPUFs making determinations on Screens and Evaluations, a subject matter expert in HSI is not required. However, the expectation is that it will be performed by a knowledgeable individual whose level of responsibility is commensurate with making engineering judgements on regulatory issues. Table 1 provides examples of HSI modifications.

There are three "basic HSI elements" of an HSI (this originates from NUREG-0700):

- **Displays**: the visual representation of the information personnel need to monitor and control the plant.
- **Controls**: the devices through which personnel interact with the HSI and the plant.
- **User-interface interaction and management**: the means by which personnel provide inputs to an interface, receive information from it, and manage the tasks associated with access and control of information.

Any user of the HSI must be able to accurately perceive, comprehend and respond to system information via the HSI to successfully complete their tasks. Specifically, "four generic primary tasks" have been identified to enable personnel to be able to perform an action (this originates from NUREG/CR-6947):

- Monitoring and detection (extracting information from the environment and recognizing when something changes),
- Situation assessment (evaluation of conditions),
- Response planning (deciding upon actions to resolve the situation), and
- Response implementation (performing an action).

TABLE 4.1: EXAMPLE HUMAN-SYSTEM INTERFACE MODIFICATIONS

HSI Element	Typical Modification	Description/Example
Displays	Number of Parameters	Increase/decrease in the amount of information displayed by and/or available from the HSI (e.g., combining multiple parameters into a single integrated parameter, adding additional information regarding component/system performance)
	Type of Parameters	Change to the type of information displayed and/or available from the HIS (e.g., removing information that was previously available or adding information that was previously unavailable)
	Information Presentation	Change to visual representation of information (e.g., increment of presentation modified)
	Information Organization	Change to structural arrangement of data/information (e.g., information now organized by channel/train rather than by flow-path)
Controls	Control Input	Change to the type/functionality of input device (e.g., replacement of am push button with a touch screen)
	Control Feedback	Change to the information sent back to the individual in response to an action (e.g., changing feedback from tactile to auditory)
User-Interface Interaction and Management	Action Sequences	Change in number and/or type of decisions made and/or actions taken (e.g., replacing an analog controller that can be manipulated in one step with a digital controller that must be called-up on the interface and then manipulated)
	Information/ Data Acquisition	Changes that affect how an individual retrieves information/data (e.g., information that was continuously displayed via an analog meter now requires interface interaction to retrieve data from a multi-purpose display panel)
	Function Allocation	Changes from manual to automatic initiation (or vice versa) of functions (e.g., manual pump actuation to automatic pump actuation)

To determine potential adverse impacts of HSI modifications on design functions, a two-step HFE evaluation must be performed, as follows:

- Step One - Identify the generic primary tasks that are involved with (i.e., potentially impacted by) the proposed activity.
- Step Two - For all primary tasks involved, assess if the modification adversely impacts an individual's ability to perform the generic primary task.

The HFE should take the “three basic elements of HSI” and make an engineering judgement as to whether the proposed activity could adversely impact any of the “four generic primary tasks.” Examples of impacts on an individual's performance that result in adverse effects on a design function include, but are not limited to:

- increased possibility of mis-operation,
- increased difficulty in evaluating conditions,
- increased difficulty in performing an action,
- increased time to respond, and
- creation of new potential failure modes.

Example 4-9: Screening for a Control Valve Upgrade (Screens Out)

Proposed Activity Description

Currently, a knob is rotated clock-wise to open a flow control valve on the secondary cooling system of a 500 kW TRIGA reactor in 1% increments and counter clock-wise to close a flow control valve in 1% increments. This knob will be replaced with a touch screen that has two separate arrows, each in its own function block. Using the touch screen, touching the "up" arrow will open the flow control valve in 1% increments and touching the "down" arrow will close the flow control valve in 1% increments. The touch screen is part of a PLC unit that has one input and one output, the programing functions are simple in nature, the operator cannot alter the display, and the software can be password protected. A qualitative engineering evaluation supporting this change identifies that the likelihood of failure of the software and hardware is sufficiently low. Additionally, given the inventory of primary water and low power, this is not considered a safety-related system.

The UFSAR states the operator can "open and close the flow control valve using manual controls located in the Main Control Room." Thus, the design function is the ability of the operator to manually adjust the position of the flow control valve and the UFSAR description implicitly identifies the SSC (i.e., the knob).

HFE Evaluation

STEP 1. Identification of the Generic Primary Tasks Involved:

1. Monitoring and detection (extracting information from the environment and recognizing when something changes) - NOT INVOLVED
2. Situation assessment (evaluation of conditions) - NOT INVOLVED
3. Response planning (deciding upon actions to resolve the situation) - NOT INVOLVED
4. Response implementation (performing an action) – INVOLVED

STEP 2. Assessment of Modification Impacts on the Involved Generic Primary Tasks:

Tasks 1, 2 and 3 were not involved, so these tasks are not impacted by the modification.

Task 4 is involved. The HFE evaluation determined that the change from knob to touch screen would not impact the operator's ability to perform the response implementation task.

Screen Response

Using the results from the engineering/technical information supporting the change, including the HFE evaluation, and examining the replacement of the "knob" with a "touch screen," the modification is *not adverse* (for the aspect being illustrated in this example) because it does not impact the ability of the operator to "open and close the flow control valve using manual controls located in the Main Control Room," maintaining satisfaction of how the UFSAR-described design function is performed or controlled.

Example 4-10. Screening for a Secondary Cooling System Control Upgrade (Screen Out)

Proposed Activity Description

Analog components and controls for a secondary cooling system at a 5 MW plate-type fueled research reactor are to be replaced with digital components and controls (on a touch screen), including new digital-based HSI. The secondary cooling system is considered safety-related. The touch screen is part of a PLC unit that has four inputs and four outputs, the programing functions are simple in nature, the operator cannot alter the display (non-configurable), it is easily tested, and the software can be password protected. A qualitative engineering evaluation supporting this change identifies that the likelihood of failure of the software and hardware is sufficiently low.

A review of the UFSAR, including the assumptions described in the safety analyses, determined that there were no additional design functions related to how design function (b) was performed or controlled. Namely, there were no design functions related to the number of steps necessary to perform the design function (i.e., complexity) or the duration in which the steps were to be performed (i.e., time response). UFSAR design function identified include:

a. Status indications are continuously available to the operator.

b. The operator controls the system components manually.

Currently, a channel/train of information and controls are provided to the operators in the Main Control Room. For the channel/train, several different analog instruments present information regarding the performance of the system. The analog displays are arranged by system "flow path" to facilitate the operator's ability to monitor the system as a whole.

The existing HSI for these components is made up of hard-wired switches, indicator lights and analog meters. The new HSI consolidates the information and controls onto a flat panel display with touch screen “soft” controls. The information available on the flat panel is equivalent to that provided on the current analog HSI. The flat panel display contains only one screen that displays the information and the controls for only that train, replicating the information and controls arrangement as they are in the existing HSI.

The existing HSI requires operators to manipulate analog switches to implement a control action. To take a control action using the new HSI, the operator must (via the touch screen) select the appropriate activity (e.g., starting/initiating the system or changing the system line-up), select the component to be controlled (e.g., pump or valve), select the control action (e.g., start/stop or open/close) and execute the action.

HFE Evaluation

Step 1. Identification of Which Four Generic Primary Tasks are Involved:

1. Monitoring and detection (extracting information from the environment and recognizing when something changes) – INVOLVED

2. Situation assessment (evaluation of conditions) – NOT INVOLVED

3. Response planning (deciding upon actions to resolve the situation) –NOT INVOLVED

4. Response implementation (performing an action) – INVOLVED

Step 2. Assessment of the Modification Impacts on the Involved Generic Primary Tasks:

Task 1 is involved. Any change to information presentation has the potential to impact the operator’s ability to monitor and detect changes in facility parameters. Even though the modification will result in information being presented on a flat panel, the information available and the organization of that information (e.g., by train) will be equivalent to the existing HSI. Due to this equivalence and additional favorable factors (e.g., appropriately sized flat panels, appropriate display brightness, clearly identified function buttons, etc.), as documented in the HFE evaluation, there is no impact on the operator’s ability to monitor and detect changes in plant parameters.

Tasks 2 and 3 were not involved, so these tasks are not impacted by the modification.

Task 4 is involved. The modification will require the operator to perform four actions in order to manipulate a control (i.e., 1. select the appropriate activity, 2. select the specific component to be controlled, 3. select the control action to be initiated, and 4. execute the action). However, this is essentially duplicated by the digital display with graphical icons representing each component. The HFE

evaluation determined that the modification impacts the operator's ability to respond by requiring four actions instead of one action and the additional actions result in an increase in the operator's time to respond. However, the HFE evaluation concluded that the operator actions continue to take place and can be performed in a timely and comparable manner.

Screen Response

Since the information available and the organization of that information using the new HSI is equivalent to the existing HSI, the design function for continuous availability of status indications is met and there is *no adverse* impact (for the aspect being illustrated in this example) on design function (a).

Using the touch screen, the operator is still able to perform design function (b) to manipulate the control for the systems components. Therefore, there is *no adverse* impact (for the aspect being illustrated in this example) on how design function (b) is performed or controlled because the HFE evaluation concluded that the operator actions continue to take place and could be performed in a timely and comparable manner.

Example 4-11. Screening for a Secondary Cooling System Control Upgrade (Screens In)

Proposed Activity Description

Analog components and controls for a secondary cooling system at a 10 MW plate-type fueled research reactor are to be replaced with digital components and controls (on a touch screen), including new digital-based HSI. The secondary cooling system is considered safety-related. The touch screen is part of a PLC unit that has four inputs and four outputs, the programing functions are simple in nature, it is non-configurable to the operator, it is easily tested, and the software can be password protected. A qualitative engineering evaluation supporting this change identifies that the likelihood of failure of the software and hardware is sufficiently low.

A review of the UFSAR, including the assumptions described in the safety analyses, determined that there were no additional design functions related to how design function was performed or controlled. Namely, there were no design functions related to the number of steps necessary to perform the design function (i.e., complexity). UFSAR design function identified include:

a. Status indications are continuously available to the operator.

b. The operator controls the system components manually.

However, the review of the UFSAR, including the assumptions described in the safety analysis, determined that an additional design function related to *how* design function was performed exists. Namely, in the pertinent safety analysis, a response time requirement of the operator had been credited.

Currently, a channel/train of information and controls are provided to the operators in the Main Control Room for the systems. Several different analog instruments present information regarding the performance of the system. The analog displays are arranged by system "flow path" to facilitate the operator's ability to monitor the system as a whole.

The existing HSI for these components is made up of redundant hard-wired switches, indicator lights and analog meters. The new HSI consolidates the information and controls onto one flat panel display with touch screen "soft" controls. The information available on the flat panel is equivalent to that provided on the current analog HSI. The flat panel display contains only one screen, which can display the information for only one train and the controls for only that train, replicating the information and controls arrangement as they are in the existing HSI. The flat panel display can be *customized* to display the parameters and/or the configuration (e.g., by flow path or only portions of a train or flow path) preferred by the operators. In addition, the flat panel displays provide many other display options to the user (e.g., individual component status and component/system alarms).

The existing HSI requires operators to manipulate analog switches to implement a control action. To take a control action using the new HSI, the operator must (via the touch screen) select the appropriate activity (e.g., starting/initiating the system or changing the system line-up), select the component to be controlled (e.g., pump or valve), select the control action (e.g., start/stop or open/close), and execute the action.

HFE Evaluation

Step 1. Identification of Which Four Generic Primary Tasks are Involved:

1. Monitoring and detection (extracting information from the environment and recognizing when something changes) – INVOLVED

2. Situation assessment (evaluation of conditions) – INVOLVED

3. Response planning (deciding upon actions to resolve the situation) –INVOLVED

4. Response implementation (performing an action) – INVOLVED

Step 2. Assessment of the Modification Impacts on the Involved Generic Primary Tasks:

Tasks 1, 2 and 3 are involved (emphasizing that the modification includes a change to information presentation and organization, such that the indications/instruments are now consolidated and presented on *customizable* flat panel displays, rather than static analog control boards). With the new displays and display options available to the operators, the operators can choose which parameters to display and the organization of that information (e.g., by train/path). The HFE evaluation concluded that this modification could result in the operator choosing not to have certain parameters displayed; thus, impacting their ability to monitor the plant and detect changes. In addition, altering the information displayed and the organization of the information will impact the operator's understanding of how the information relates to system performance. This impact on understanding will also impact the operator's ability to assess the situation and plan an appropriate response.

Task 4 is involved. The modification will require the operator to perform four actions in order to manipulate a control through a pulldown menu (i.e., 1. select the appropriate activity, 2. select the specific component to be controlled, 3. select the control action to be initiated, and 4. execute the action). Currently, the operator is able to manipulate a control in one action (e.g., turn a switch to *on/off*). The HFE evaluation determined that the modification impacts the operator's ability to respond by requiring four actions instead of one action and the additional actions result in an increase in the

operator's time to respond. However, the HFE evaluation concluded that due to the pulldown menu the operator actions will take a marginal amount of time longer to perform the action.

Screen Response

The information available and the organization of that information in the new displays are *customizable* based on operator preference. Critical status indications may not be continuously available to the operator, thus there is an *adverse* impact (for the aspect being illustrated in this example) on the design function.

Using the touch screen, the operator is still able to perform design function to manipulate the control for the systems components. However, there is also an *adverse* impact (for the aspect being illustrated in this example) on how design function is performed due to the increased response time because the HFE evaluation concluded that the operator actions will take longer to perform.

Example 4-12. Screening for a Recorder Upgrade (Screens In)

Proposed Activity Description

An analog recorder is to be replaced with a new microprocessor-based recorder. The recorder is used to display data on the airborne radioactive material monitoring system within the reactor bay. The analog recorder is a simple ink strip chart showing a waterfall display. An engineering/technical evaluation performed on the change determined that the new recorder will be highly dependable (based on a quality development process, testability, and successful operating history) and therefore, the risk of failure of the recorder due to software is considered very low. The new recorder also meets all current required performance and qualification requirements, and would introduce no new failure modes or effects at the level of the design function. The operator will use the new recorder in the same way the old one was used. However, the display will provide the current value of both the particular and gas channels, rather than show them in a waterfall display like the current analog strip-chart recorder does.

The USFAR-described design function of the airborne radioactive material monitoring system is to measure the amount of particulate and gaseous radioactive material in the reactor bay air, alarm on a high-level condition, and initiate a shutdown of the ventilation system upon a high-level condition.

HFE Evaluation

Step 1. Identification of Which Four Generic Primary Tasks are Involved:

1. Monitoring and detection (extracting information from the environment and recognizing when something changes) – INVOLVED

2. Situation assessment (evaluation of conditions) – INVOLVED

3. Response planning (deciding upon actions to resolve the situation) –INVOLVED

4. Response implementation (performing an action) – NOT INVOLVED

Step 2. Assessment of the Modification Impacts on the Involved Generic Primary Tasks:

Tasks 1, 2 and 3 are involved. The modification will require that the operator read, assess, and decide upon a course of action for a response based upon not only how high the values are but also how fast the values are changing. Small changes in the rate-of-rise might reflect ambient weather conditions affecting background while large changes could indicate fission product release from fuel.

Task 4 is likely not involved. The performance of the action is unaffected once the course of action from Step 3 is determined.

Screen Response

The activity is *adverse* on the design function of the airborne radioactive material monitoring system because the method of display has significantly changed. A waterfall display allows the operator to have a better understanding almost instantly of how fast the parameters are changing. While this type information could also be obtained from watching the instantaneous data (i.e., single value for each channel) changing over time, some ability to rapidly determine trends is lost. For example, it may not be intuitive to determine linear or exponential changes in the data. The licensee concludes that the change could potentially adversely affect how the operator interprets data being displayed and screens in the change.

4.2.2.7 Screening Changes to UFSAR Methods of Evaluation

By definition, a proposed activity involving a digital modification involves SSCs and how SSCs are operated and controlled, is not a ***method of evaluation*** described in the UFSAR (see NEI 21-06, Rev. 1, Section 3.10).

Methods of evaluation are analytical or numerical computer models used to determine and/or justify conclusions in the UFSAR (e.g., accident analyses that demonstrate the ability to safely shut down the reactor or prevent/limit radiological releases). These models also use "software." However, the software used in these models is separate and distinct from the software installed within hardware in the facility. The response to this screen consideration should reflect this distinction.

A necessary revision or replacement of a method of evaluation resulting from a digital modification is separate from the digital modification itself and the guidance in NEI 21-06, Rev. 1, Section 4.2.1.3 applies.

4.2.3 Is the Activity a Test or Experiment Not Described in the UFSAR?

By definition, a proposed activity involving a digital modification involves SSCs and how SSCs are operated and controlled, is not a ***test or experiment*** (see NEI 21-06, Rev. 1, Section 3.14). The response to this Screen consideration should reflect this characterization.

A necessary test or experiment involving a digital modification is separate from the digital modification itself and the guidance in NEI 21-06, Rev. 1, Section 4.2.2 applies.

4.3 Evaluation

There are eight 10 CFR 50.59 evaluation criteria in the form of questions. This document provides general guidance on addressing each question with respect to digital upgrades. Supplemental guidance specific to digital upgrades is clearly needed due to complexity introduced by software. The eight questions are:

1. Does the activity result in more than a minimal increase in the frequency of occurrence of an accident?

2. Does the activity result in more than a minimal increase in the likelihood of occurrence of a malfunction of an SSC important to safety?

3. Does the activity result in more than a minimal increase in the consequences of an accident?

4. Does the activity result in more than a minimal increase in the consequences of a malfunction?

5. Does the activity create a possibility for an accident of a different type?

6. Does the activity create a possibility for a malfunction of an SSC important to safety with a different result?

7. Does the activity result in a design basis limit for a fission product barrier being exceeded or altered?

8. Does the activity result in a departure from a method of evaluation described in the UFSAR used in establishing the design bases or in the safety analyses?

Illustrated in Figure 4.2, digital modifications usually are only involved in four of the eight questions. This is due to the fact that software is unlikely to affect consequences (i.e., dose to the general public), not usually involved with fission product barriers, and the use of software for calculations is handled separately from what was intended with digital modifications.

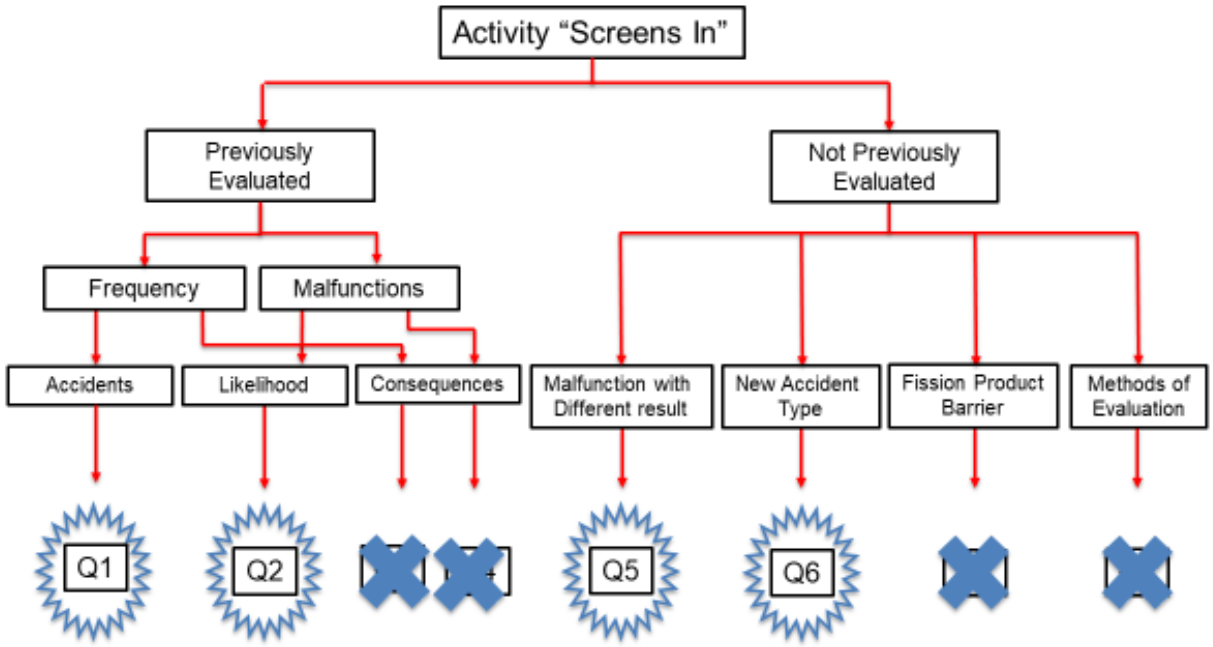

Figure 4.2: Flow path of the Evaluation process for digital modifications leading to the eight evaluation questions.

If the evaluation shows that any of the 10 CFR 50.59 criteria are not met, the licensee submits a license amendment request to the NRC and needs to receive approval prior to implementation. If the modification uses a design that was approved previously by the NRC or references a design previously approved by a topical report evaluation, the submittal should focus on application-specific features (i.e., conditions of approval identified in the NRC Safety Evaluation Report) or differences from the previously approved implementation.

4.3.1 Does the Activity Result in More Than a Minimal Increase in the Frequency of Occurrence of an Accident?

For purposes of 10 CFR 50.59, both Anticipated Operational Occurrences (AOOs) and Postulated Accidents (PAs) fall within the definition of "accident."

The first step in addressing this criterion is to identify the accidents that have been evaluated in the UFSAR and that may be affected by the proposed activity. Then the change is evaluated to determine whether the frequency of these accidents could increase as a result of the change. In answering this question for digital upgrades, the key issue is whether the digital equipment can increase the frequency of initiating events that lead to accidents, considering the following:

- Does the system automate some aspect of plant operation that could relate to accident initiators?
- Does the system exhibit performance or dependability characteristics that increase the need for operator intervention or increase operator burden to support operation of the system in normal or off-normal conditions?

- Could this increase the probability of an accident previously evaluated?

All initiating events fall into one of two categories: equipment-related or personnel-related. Therefore, the assessment of the impact of a digital modification also needs to consider both equipment-related and personnel-related sources.

For a digital modification, the range of possible equipment-related sources of initiating events includes items unique to digital and items not unique to digital. An example of an item unique to digital is consideration of the impact on accident frequency due to a software CCF. An example of a potential source of CCF that is not unique to digital is consideration of the impact on accident frequency due to the digital system's compatibility with the environment in which the system is being installed.

4.3.1.1 Factors that Effect Reliability

To support the licensing and 10 CFR 50.59 process, methods are needed to evaluate digital system quality and the likelihood of failure. For hardware, methods are well established for estimating reliability or probability of hardware failure. However, for software there are no well-established, accepted quantitative methods that can be used to estimate reliability, particularly for the high levels of reliability required of safety-critical software. Without such methods, other means must be used to gain reasonable assurance that the quality of the design is adequate. The answer lies in evaluation of the process used to develop the software, and characteristics of the resulting design. Although accepted methods for estimating software reliability are not presently available, there are well-established methods and engineering processes for development, evaluation, and control of software that can be used to produce highly dependable, high-quality digital systems.

In this guideline, the term dependability is used in relation to quality and likelihood of failures. This term reflects the fact that reasonable assurance of adequate quality and low likelihood of failure is derived from a qualitative assessment of the design process and the system design features. The term dependability also reflects the importance of ensuring that the system performs its functions in a consistent and repeatable manner and its behavior is predictable. A reliable system that performs its intended function, but exhibits other undesirable behavior, is not dependable.

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:

- The development and quality assurance processes implemented for both the digital platform and the plant-specific application software. Compliance with appropriate industry standards and regulatory guidelines for development, software safety analysis, V&V, and configuration control should be demonstrated.

- Hardware and software design features that contribute to high dependability. Such 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.

The safety significance and simplicity of the system also play a role in assurance of quality and dependability. Software development activities need to be more rigorous for applications that have high safety significance. Systems that are sufficiently simple have more well-defined failure modes and tend

to allow for more thorough testing of all input and output combinations than complex systems; complexity increases the uncertainty associated with demonstrating software quality.

In addition, the maturity of the product and in-service experience with the platform and the plant system application should be considered. Substantial applicable operating history reduces uncertainty in demonstrating adequate dependability. Credit should also be taken for using digital platforms that have previously been reviewed by the NRC as part of generic qualification for safety-related applications.

The final determination of dependability and likelihood of failures should 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 dependability that helps compensate for a lack of operating history.

Even when appropriate design processes are followed in developing software and digital systems, because of the lack of well-established methods for estimating reliability or dependability, there still is some residual uncertainty when evaluating the potential for software errors to defeat safety functions in redundant, safety-related channels or result in faults in non-diverse uses of the same software (whether safety or non-safety related). Consequently, for certain safety system upgrades, particularly safety channels and engineered safety features, the NRC expects that a formal analysis will be performed to demonstrate that adequate defense-in-depth and diversity is provided to cope with postulated accidents in the presence of common cause failures.

4.3.1.2 Qualitative Assessments

Facilities may use PRA calculations to assess the change in probable frequency of events. Note that "more than a minimal increase" means greater than 10 percent for PRA calculations. However, PRA data or any numerical values qualifying an accident frequency are unlikely to be available for an NPUF. Therefore, a more qualitative approach is used in the form of an engineering evaluation called a Qualitative Assessment.

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

The purpose of the Qualitative Assessment is to determine whether an increase in frequency "is more than minimal" or if it can reasonably be determined at all. There are two outcomes from a qualitative assessment:

- If the *qualitative assessment outcome* is **sufficiently low**, then there is NOT more than a minimal increase in the frequency of occurrence of an accident previously evaluated in the UFSAR.

- If the *qualitative assessment outcome* is **not sufficiently low**, then there may be more than a minimal increase in the frequency of occurrence of an accident previously evaluated in the UFSAR.

There are five terms that should be used to make a determination in the context of determining what is minimal:

1. **Better**: If the change results in something that is better, in other words lowers the frequency of an accident, then the change is clearly less than minimal.

2. **Zero**: There is no change in the frequency of an accident or malfunction.

3. **Negligible**: To achieve a negligible conclusion, the change in the accident frequency *"...is so small or the uncertainties in determining whether a change in frequency has occurred are such that it cannot be reasonably concluded that the frequency has actually changed (i.e., there* is no clear trend toward increasing the frequency)". This implies that the uncertainties are small compared to the magnitude of the change.

4. **Discernable**: If a clear trend towards increasing the accident frequency exists, then a *discernable* increase in the accident frequency would exist. When taking into account uncertainty, this implies that the change is statistically significant but that the uncertainties are also reasonably small compared to the magnitude of the change.

5. **Significant**: The change in frequency is clearly significant.

In this case, the Qualitative Assessment (and/or any other supporting information) should be used to assess the qualitative increase in the magnitude of the accident frequency and determine if the discernable increase in the accident frequency is "more than minimal" or "NOT more than minimal."

Figure 4.3 illustrates the relationship between these key words and the 50.59 process. In the range of better, zero, or negligible, the change is not more than minimal, or it can't be reasonably be determined to have changed. A Qualitative Assessment would conclude that the increase in frequency of occurrence of an accident is sufficiently low. Evaluations are used to make a determination in the murky area between negligible and discernable (i.e., a change in frequency has occurred but it is not discernable). If the determination is that the increase in frequency of an accident is not discernable, then the conclusion would be that frequency of an accident is sufficiently low. If the determination is that the increase in frequency of an accident is discernable as a result of the change, then the conclusion of the Qualitative Assessment would be that frequency of an accident is not sufficiently low. A license amendment is the appropriate pathway for situations where the increase in the frequency of occurrence of an accident is discernable, regardless of magnitude.

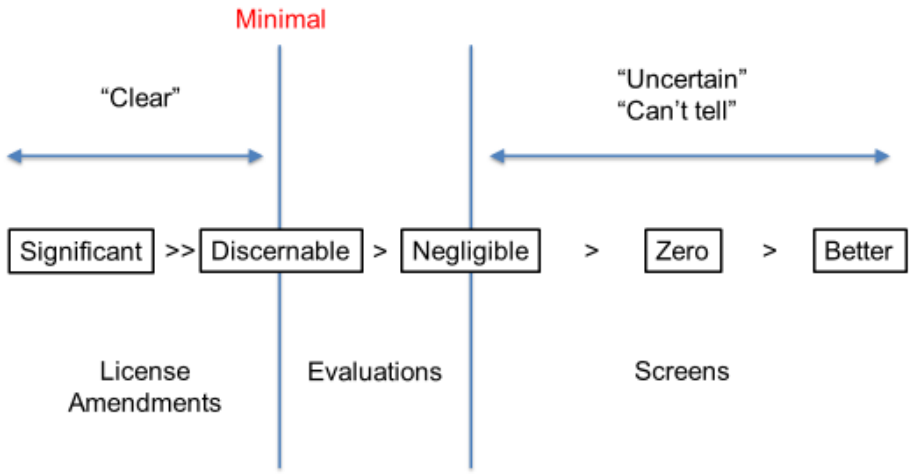

Figure 4.3: Relationship Between the Key Words Used in a Qualitative Assessment and in the 10 CFR 50.59 Process

As part of the assessment to determine the qualitative increase in the magnitude of the accident frequency, the concept of interdependence also needs to be considered and applied. Namely, interdependence considers the overall impact due to the change. For example, the "negative" impact due to a software CCF likelihood being **not sufficiently low** could be partially or wholly offset by the "positive" impacts due to the digital system/component itself and/or its design features.

To achieve a conclusion of "NOT more than minimal" based on the engineering/technical information supporting the change, the proposed activity must also continue to meet and/or satisfy all applicable NRC requirements, as well as design, material, and construction standards to which the licensee is committed. Applicable requirements and standards include those selected by the licensee for use in the development of the proposed digital modification and documented within the design modification package.

Because these determinations are qualitative in nature, it is important that the logic used to arrive at a particular judgement is clearly documented. Remember, such judgments may be difficult to duplicate and understand at a later time. As such, the basis for the engineering judgment and the logic used in the determination should be documented to the extent practicable. This type of documentation is of particular importance in areas where no established consensus methods are available, such as for software reliability, or the use of commercial-grade hardware and software where full documentation of the design process is not available.

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

- replacement of analog relays (including timing relays) with digital relays
- replacement of analog controls for safety-related support systems such as chiller (heating, ventilation, and air conditioning) systems and lubricating oil coolers

- replacement of analog controls for emergency diesel generator supporting systems and auxiliary systems such as voltage regulation
- installation of circuit breakers that contain embedded digital devices
- replacement of analog recorders and indicators with digital recorders and indicators
- digital upgrades to non-safety related control systems

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

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

Finally, due to the level of quality, rigor, and expertise required to meet the expectations of determining the appropriateness of making a digital modification under 10 CFR 50.59 to reactor safety systems, use of Qualitative Assessments for important safety-related SSCs, such as safety channels or ESFAS, is not appropriate.

4.3.1.3 Qualitative Assessments: Design Attributes

Design attributes of a proposed modification can prevent or limit failures from occurring. Design attributes focus primarily on built-in features such as fault detection and failure management schemes, internal redundancy, and diagnostics within the integrated software and hardware architecture. However, design features external to the proposed modification (e.g., mechanical stops on valves or pump speed limiters) may also be considered.

Many system design attributes, procedures, and practices can contribute to significantly reducing the likelihood of failure (e.g., CCF). A licensee can account for this by assessing the specific vulnerabilities through postulated failure modes (e.g., software CCF) within a proposed modification and applying specific design attributes to address those vulnerabilities. An adequate qualitative assessment of the likelihood of failure of a proposed modification would describe the potential failures that the proposed modification could introduce and the specific design attributes incorporated to resolve the identified potential failures. It would also explain how the chosen design attributes and features resolve the identified potential failures.

Diversity is one example of a design attribute that licensees can use to demonstrate that an SSC modified with digital technology is protected from a loss of design function caused by a potential CCF. In

some cases, a plant's design basis may specify diversity as part of the design. In other cases, licensees do not need to consider the use of diversity in evaluating a proposed modification. Diversity within the proposed design can be a powerful means for significantly reducing the occurrence of failures that affect the accomplishment of design functions.

4.3.1.4 Qualitative Assessments: Quality of the Design Process

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

Such processes include software development, hardware and software integration processes, system design, and validation and testing processes that have been incorporated into development. For safety-related digital equipment composed of integrated hardware and software, this development process would be documented and available for referencing in the qualitative assessment for proposed modifications. However, for commercial-grade-dedicated or non-safety related digital equipment comprising integrated hardware and software, documentation of the development process may not be as extensive. In such cases, the qualitative assessment may place greater emphasis on the design attributes included and the extent of successful operating experience for the equipment proposed.

The quality of the design process for non-commercial-grade-dedicated software or hardware (e.g., software or hardware developed in-house) is a key element in determining the dependability of the proposed modifications. When possible, the use of applicable industry consensus standards contributes to a quality design process and provides a previously established acceptable approach (e.g., Institute of Electrical and Electronics Engineers (IEEE) Standard (Std.) 1074-2006, "IEEE Standard for Developing a Software Project Life Cycle Process," which is endorsed in Regulatory Guide 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plant"). In some cases, other nuclear or nonnuclear standards can also provide technically justifiable approaches for use if they apply to the specific application.

Quality standards should not be confused with quality assurance programs or procedures. Quality standards are those standards that describe the benchmarks that are specified to be achieved in a design. Quality standards should be documents that are established by consensus and approved by an accredited standards development organization. For example, IEEE is a recognized standards development organization that publishes consensus-based quality standards that are relevant to digital I&C modifications. Quality standards used to ensure that a quality design process was used to develop the proposed change need not be limited to those endorsed by the NRC staff. The qualitative assessment document should demonstrate that the standard being applied is valid under the circumstances for which it is being used. For NPUFs, an acceptable quality assurance standard is ANS/ANSI 15.8 (R2018), "Quality Assurance Program Requirements for Research Reactors."

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

4.3.1.5 Qualitative Assessment: Operating Experience

Relevant operating experience can be used to help evaluate and demonstrate that integrated software and hardware equipment employed in a proposed modification has adequate dependability. The licensee may document information showing that the proposed system or component modification uses equipment with significant operating experience in nuclear power plant applications or in nonnuclear applications with comparable performance standards and operating environment. The licensee may also consider whether the suppliers of such equipment incorporate quality processes such as continual process improvement and incorporation of lessons learned and document how that information demonstrates adequate equipment dependability.

Differences may exist in the specific digital I&C application between the proposed digital I&C modification and that of the integrated hardware and software whose operating experience is being credited. In all cases, however, the architecture of the referenced equipment and software should be substantially similar to that of the proposed system.

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

Example 4-13. Recorder Upgrade (NOT MORE THAN A MINIMAL increase in the frequency of occurrence of an accident previously evaluated in the UFSAR)

Proposed Activity Description

An analog recorder is to be replaced with a new microprocessor-based PLC recorder. The recorder is used to display data on the airborne radioactive material monitoring system within the reactor bay. The analog recorder is a simple ink strip chart showing a waterfall display. An engineering/technical evaluation performed on the change determined that the new recorder will be highly dependable (based on a quality development process, testability, and successful operating history) and therefore, the risk of failure of the recorder due to software is considered sufficiently low. The new recorder also meets all current required performance, and qualification requirements, and would have no new failure modes or effects at the level of the design function. The operator will use the new recorder in the same way the old one was used (e.g., display only; no alarming function). However, the display will provide the current value of both the particulate and gas channels, rather than show them in a waterfall display like the current analog strip-chart recorder does.

The USFAR-described design function of the airborne radioactive material monitoring system is to measure the amount of particulate and gaseous radioactive material in the reactor bay air, alarm on a high-level condition, and initiate an automatic shutdown of the ventilation system upon a high-level condition.

Qualitative Assessment Outcome

The qualitative assessment considered system design attributes, quality of the design processes employed, and the operating experience of the proposed equipment. The frequency of failure of the proposed digital recorder is much lower than the existing recorder. It was determined though that a failure of the recorder does not impact the frequency of occurrence of an accident as the failure of either the analog or digital recorder would not affect the ability for the monitoring system to perform its design function. Therefore, it was concluded that the failure likelihood introduced by the modified SSC is sufficiently low.

Conclusion

With the failure likelihood introduced by the modified SSC being sufficiently low, there is not more than a minimal increase in the frequency of occurrence of an accident previously evaluated in the UFSAR.

Example 4-14. Secondary Pump Control System Upgrade With Existing Unknown Failure Rate (NOT MORE THAN A MINIMAL Increase in the Frequency of Occurrence of an Accident)

Proposed Activity Description

A 5-MW research reactor has two safety-related redundant secondary pumps, each with its own flow control valve. There are two analog control systems (one per pump and flow control valve combination) that are physically and functionally the same. Each analog control system will be replaced with a separate digital control system. The hardware platform for each digital control system is from a different supplier and the software in each digital control system is unique. Engineering/technical information supporting the change showed that each digital control system was from a reputable manufacture, made under a quality control plan (although not a 10 CFR 50, Appendix B, QA plan), was very simple in nature (one input and two outputs), has a self-test and self-diagnostic capability, not configurable, and easily tested. Neither of the analog controllers have ever failed in their 31 years of operation but they are obsolete. As part of an aging management plan, there is a desire to update these controllers. The manufacturers estimation of mean time between failure (MTBF) for the new control systems were 23 and 35 years during continuous operation, respectively.

Qualitative Assessment Outcome

The qualitative assessment considered system design attributes, quality of the design processes employed, and the operating experience of the proposed equipment. Detailed or specific information on the frequency of failure of the current analog control system was not known/available and the manufacturer is no longer in business. It was determined that although the true change between the MTBF of the current system and the new systems were unknown, it was reasonable to conclude that the difference was at least negligible for each new digital system given the long lives of the equipment involved, and concluded that the failure likelihood introduced by the modified SSC is sufficiently low.

Conclusion

With the failure likelihood introduced by the modified SSC being sufficiently low, there is not more than a minimal increase in the frequency of occurrence of an accident previously evaluated in the UFSAR.

4.3.2 Does the Activity Result in More Than a Minimal Increase in the Likelihood of Occurrence of a Malfunction of an SSC Important to Safety?

After applying the generic guidance in NEI 21-06, Rev. 1, Section 4.3.2 to identify any malfunctions affected by the systems/components involved with the digital modification, the change is examined to determine if the likelihood of these malfunctions could increase due to the change. When addressing this evaluation criterion for digital upgrades, the key issue is determining if the digital equipment can increase the likelihood of initiating events that lead to the identified malfunctions.

All initiating events fall into one of two categories: equipment-related or personnel-related. Therefore, the assessment of the impact of a digital modification also needs to consider both equipment-related and personnel-related sources.

For a digital modification, the range of possible equipment-related sources of initiating events includes items unique to digital and items not unique to digital. An example of an item unique to digital is consideration of the impact on malfunction likelihood due to a software CCF, which will be addressed in this guidance. An example of a potential source of common cause failure that is not unique to digital is consideration of the impact on malfunction likelihood due to the digital system's compatibility with the environment in which the system is being installed.

Typically, numerical values quantifying a malfunction likelihood are not available at NPUFs. Furthermore, a failure modes and effects analysis is also typically not performed as part of the licensing process at NPUFs. Alternatively, a qualitative approach is taken through a Qualitative Assessment previously described.

In the context of this question, the SSC under consideration depends on the level of detail described in the UFSAR. If the relevant design functions are described in terms of the system in which the digital device is installed, then the system is the SSC. If the UFSAR describes the design functions in terms of the component that the digital device is replacing, then the new digital device is the SSC under consideration in this question.

The likelihood of occurrence of a malfunction of an SSC important to safety is directly related to the likelihood of failure of equipment that causes a failure of SSCs to perform their intended design functions [e.g., an increase in the likelihood of failure of an ECCS drain valve has a corresponding increase in the likelihood of occurrence of a malfunction of SSCs (i.e., the ECCS valve vs. the ECCS system)]. Thus, an increase in the likelihood of failure of the modified subcomponent that causes the failure of an SSC to perform its intended design functions is directly related to the likelihood of the occurrence of a malfunction of an SSC important to safety. Therefore, if the Qualitative Assessment outcome is “sufficiently low,” the activity does not result in more than a minimal increase in the likelihood of occurrence of a malfunction of an SSC important to safety previously evaluated in the UFSAR.

Digital modifications that involve networking; combining design functions from different systems; interconnectivity across channels, systems, and divisions; or shared resources, merit careful review to determine if such modifications cause reductions in the redundancy, diversity, separation, or independence of UFSAR-described design functions. In general, changes that reduce the UFSAR credited level of system/equipment redundancy, diversity, separation or independence do not meet the minimal threshold for this question and require NRC approval. However, licensees may reduce excess

redundancy, diversity, separation or independence (if any) to the level credited in the UFSAR without prior NRC approval.

Evaluations of the dependability of the system are needed to assess whether the likelihood of malfunctions has increased. In many cases, digital upgrades are installed to replace obsolete and/or unreliable equipment that has become costly to maintain. If actual failure rate data are available for the old equipment and the replacement equipment, it may be used to evaluate the change in hardware reliability. Typically, digital hardware is more reliable than the equipment it replaces. Also, modern digital equipment designed for safety significant applications often incorporates important design features that contribute to a lower likelihood of malfunction. Such features can improve the dependability of a train of a system; thus, preserving the system-level design function. These features should be credited in the 10 CFR 50.59 evaluation, and may include:

Internal redundancy and fault tolerance to preclude single faults from causing the device to malfunction.

- Self-diagnostics to detect and alarm faults, or abnormal or unanticipated conditions so that operators can take timely corrective action before the system is called upon to perform its design function. Of course, good self-diagnostics should be coupled with an effective corrective action program at the facility.

- Self-test routines that perform surveillance testing functions on a more frequent basis than the original, manually executed surveillance tests.

While it is expected that newer equipment will be more reliable than the equipment it is replacing, other issues that should be addressed are compliance with applicable regulations and industry standards; qualification for environmental conditions (seismic, temperature, humidity, radiation, pressure, and EMC); performance requirements for the plant-specific application; proper design of electrical power supplies; cooling or ventilation for thermal loads; and separation, independence and grounding.

Example 4-15. Secondary Pump Control System Upgrade with Known Existing Failure Rate (NOT MORE THAN A MINIMAL Increase in the Likelihood of Occurrence of a Malfunction of an SSC Important to Safety)

Proposed Activity Description

A 5-MW research reactor has two safety-related redundant secondary pumps, each with its own flow control valve. There are two analog control systems (one per pump and flow control valve combination) that are physically and functionally the same. Each analog control system will be replaced with a separate digital control system. The control systems are not described in the UFSAR. However, the higher-level system that is affected in the secondary cooling system with the design bases function of removing heat from the primary cooling system through a heat exchanger.

The hardware platform for each digital control system is from a different supplier and the software in each digital control system is unique. Engineering/technical information supporting the change showed that each digital control system was from a reputable manufacture, made under a quality control plan (although not a 10 CFR 50, Appendix B, QA plan), was very simple in nature (one input and two outputs), has a self-test and self-diagnostic capability, was not configurable, and easily tested. One of the current analog control systems has recently failed after 22 years of operation but both are showing age. The

manufacturers estimation of mean time between failure (MTBF) for the new control systems were 23 and 35 years during continuous operation, respectively.

Qualitative Assessment Outcome

The qualitative assessment considered system design attributes, quality of the design processes employed, and the operating experience of the proposed equipment. Detailed or specific information on the frequency of failure of the current analog control system was not known/available and the manufacturer is no longer in business. It was determined that although the true change between the MTBF of the current system and the new systems were unknown, it was reasonable to conclude that the difference was at least negligible for each new digital system, and it was concluded that the failure likelihood introduced by the modified SSC is sufficiently low.

Conclusion

With the failure likelihood introduced by the modified SSC being sufficiently low, there is not more than a minimal increase in the frequency of occurrence of a malfunction of an SSC important to safety.

Example 4-16. Identical Secondary Pump Control System Upgrade (MORE THAN A MINIMAL Increase in the Likelihood of Occurrence of a Malfunction of an SSC Important to Safety)

Proposed Activity Description

A 5-MW research reactor has two safety-related redundant secondary pumps, each with its own flow control valve. There are two analog control systems (one per pump and flow control valve combination) that are physically and functionally the same. Each analog control system will be replaced with a separate digital control system. The control systems are not described in the UFSAR. However, the higher-level system that is affected is the secondary cooling system, with the design bases function of removing heat from the primary cooling system through a heat exchanger.

The hardware platform for each digital control system is from the same manufacturer and the software in each digital control system is identical (i.e., same make and model). Engineering/technical information supporting the change showed that the digital control system was from a reputable manufacture, made under a quality control plan (although not a 10 CFR 50, Appendix B, QA plan), had an understandable architecture (neither simple nor complex), has a self-test and self-diagnostic capability, and was tested for all the outcomes thought possible. One of the current analog control systems has recently failed after 12 years of operation but both are obsolete. The manufacturers estimation of mean time between failure (MTBF) for the new control systems was 25 years during continuous operation.

Qualitative Assessment Outcome

The qualitative assessment considered system design attributes, quality of the design processes employed, and the operating experience of the proposed equipment. Detailed or specific information on the frequency of failure of the current analog control system was not known/available and the manufacturer is no longer in business. It was determined that although the true change between the MTBF of the current system and the new systems were unknown, it was reasonable to conclude that the difference was at least negligible for each new digital system. However, because the same software

exists in both systems, a possibility for a software CCF has been introduced due to the complexity of the architecture, and concluded that the failure likelihood introduced by the modified SSC is not sufficiently low.

Conclusion

With the failure likelihood introduced by the modified SSC being not sufficiently low, there is more than a minimal increase in the frequency of occurrence of a malfunction of an SSC important to safety. A license amendment would be required.

4.3.3 Does the Activity Result in More Than a Minimal Increase in the Consequences of an Accident?

There is no unique guidance applicable to digital modifications for responding to this evaluation criterion because the identification of affected accidents and dose analysis inputs and/or assumptions are not unique for a digital modification. The guidance in NEI 21-06, Rev. 1, Section 4.3.3 applies. However, this assumes the testing confirms the applicable scaling factors for any digital modification have been implemented properly. For example, a primary digital display used by the operator to adhere to license power limits can affect the steady state flux levels, and thus assumptions on fission product inventory have the potential to be affected. While it is unlikely that an NPUF is operating that close to an input assumption in the dose analysis due to the <24/7 operational tempo of most NPUFs, it should at least be addressed in response to this question.

4.3.4 Does the Activity Result in More Than a Minimal Increase in the Consequences of a Malfunction?

There is no unique guidance applicable to digital modifications for responding to this evaluation criterion because the identification of the affected malfunctions and dose analysis inputs and/or assumptions are not unique for a digital modification. The guidance in NEI 21-06, Rev. 1, Section 4.3.4 applies. However, this assumes the testing confirms the applicable scaling factors for any digital modification have been implemented properly. For example, a primary digital display used for stack monitoring during an emergency could affect timeliness of credited actions, and thus result in a more than minimal increase in dose consequences.

4.3.5 Does the Activity Create a Possibility for an Accident of a Different Type?

When addressing this question, the types of accidents that have been evaluated in the UFSAR need to be identified and a determination made as to whether the proposed activity could create accidents that are not bounded by UFSAR-evaluated accidents. The evaluation should consider whether the change creates new events that can initiate accidents that are of a different type than those evaluated in the UFSAR. The answers to the following questions should assist in identifying accidents of a different type:

- Have the assessments of system-level potential failure modes and effects for the new system or equipment identified any new types of system-level failure modes that could cause a different type of accident than presented in the UFSAR?

- NPUF UFSAR analyses were based on credible failure modes of the existing equipment. Does the replacement system change the basis for the most limiting scenario?

The term 'accidents' refers to the anticipated (or abnormal) operational transients and postulated design basis accidents that are analyzed to demonstrate that the facility can be operate without undue risk to the health and safety of the public. Therefore, for purposes of 10 CFR 50.59, both Anticipated Operational Occurrences (AOOs) and Postulated Accidents (PAs) fall within the definition of "accident." There are two considerations that need to be assessed when directly answering this evaluation question.

- Is the change creating an accident **as likely to happen as** an accident previously evaluated?
- Is the change creating an **accident of a different type**?

4.3.5.1 Determination of "As Likely to Happen As"

The possible accidents of a different type are limited to those that are as likely to happen as those previously evaluated in the UFSAR. The accident must be credible in the sense of having been created within the range of assumptions previously considered in the licensing basis (e.g., random single failure, loss of off-site power, etc.). A new initiator of an accident previously evaluated in the UFSAR is not a different type of accident.

A change that increases the frequency of an accident previously thought to be incredible to the point where it becomes as likely as the accidents in the UFSAR, could create the possibility of an accident of a different type. To help with this determination, a Qualitative Assessment is performed.

If the outcome of the *qualitative assessment* is **sufficiently low**, then the activity does not introduce any failures that are as likely to happen as those in the UFSAR that can initiate an accident of a different type. Therefore, the activity does not create a possibility for an accident of a different type than any previously evaluated in the UFSAR.

If the outcome of the *qualitative assessment* is **not sufficiently low**, then the activity may introduce failures that are as likely to happen as those in the UFSAR that can initiate an accident of a different type, i.e., the activity created a possibility. For these cases, this evaluation criterion also needs to consider an accident of a different type.

4.3.5.2 Determination of "Accident of a Different Type"

For cases in which the outcome of the *qualitative assessment* is **not sufficiently low**, an *accident of a different type* needs to be determined. If a revision to an existing accident analysis is to be performed, then the proposed activity does NOT create the possibility of an accident of a different type. This implies that the accident is in fact described in the USFAR but the frequency increased. This situation is covered by an earlier question. The point is that the accident is not new. If a new accident analysis is needed, then the proposed activity DOES create the possibility of an accident of a different type.

Example 4-17. Primary Pump Control System Upgrade with Existing Known Failure Rate (Does NOT Create an Accident of a Different Type)

Proposed Activity Description

A 10-MW research reactor has two safety-related redundant primary pumps, each with its own flow control valve. There are two analog control systems (one per pump and flow control valve combination) that are physically and functionally the same. Each analog control system will be replaced with a

separate digital control system. The hardware platform for each digital control system is from a different supplier and the software in each digital control system is unique. Engineering/technical information supporting the change showed that each digital control system was from a reputable manufacture, made under a quality control plan (although not a 10 CFR 50, Appendix B, QA plan), was very simple in nature (one input and two outputs), has a self-test and self-diagnostic capability, was not configurable, and easily tested. One of the analog controllers failed after 41 years of operation. As part of an aging management plan, there is a desire to update these controllers because they are obsolete. The manufacturers estimation of mean time between failure (MTBF) for the new control systems were 3 and 5 years during continuous operation given the environmental conditions they operate in, respectively.

The USFAR-described design function of the primary pumps is to remove heat from the fuel. As part of the accident analysis, it is assumed that both pumps fail as a result of either a loss of electrical power (through either loss of off-site power or disruption of the electrical distribution system within the facility) or mechanical failure of the pumps themselves (i.e., barring or impeller failure).

Qualitative Assessment Outcome

The qualitative assessment considered system design attributes, quality of the design processes employed, and the operating experience of the proposed equipment. Detailed or specific information on the frequency of failure of the current analog control system was not known/available and the manufacturer is no longer in business. It was determined that although the true change between the MTBF of the current system and the new systems were unknown, it was reasonable to conclude that the potential frequency of failure was at least discernable for each new digital system given the manufacturer's supplied information, and concluded that the failure likelihood introduced by the modified SSC is not sufficiently low.

Conclusion

With the failure likelihood introduced by the modified SSC not being sufficiently low, there is more than a minimal increase in the frequency of occurrence of an accident previously evaluated in the UFSAR. However, this accident is already enveloped by an existing UFSAR described accident, although it was initiated by a previously incredible failure. Therefore, this change would not create an accident of a different type.

4.3.6 Does the Activity Create a Possibility for a Malfunction of an SSC Important to Safety with a Different Result?

Due to the unique nature of digital modifications and the inherent complexities therein, the application of this criterion is especially important. Specifically, the unique aspect of concern is the potential for a software CCF to create the possibility for a malfunction with a different result.

This question addresses results or effects of potential system failures, and whether the effects are bounded by failures explicitly described in the UFSAR. The evaluation needs to compare results of malfunctions evaluated in the UFSAR with the results of failures that the proposed activity could create. The key issue is the effect of failures of the digital device on the system in which it is installed. 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.

Note that new types of malfunctions are not the issue. 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. As an example, a digital variable speed pump control system upgrade may add new components that can have failure modes different than the original components. Provided the end result of the control system failure is bounded by the results of malfunctions already evaluated in the UFSAR (e.g., loss of feedwater), this upgrade would not create malfunctions with a different result. Put another way, if software failure cannot cause an equipment malfunction of a different type than any previously evaluated in the safety analysis report, then this criterion is satisfied, and in the absence of other disqualifying criteria, the replacement can be performed under 10 CFR 50.59 without prior NRC approval.

It is important that the evaluation needs to consider the level of detail that was previously evaluated in the UFSAR (e.g., component versus division/train versus system level failures). 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.

The two considerations that need to be assessed when answering this evaluation question *are as likely to happen as* and the *impact on the malfunction result*.

4.3.6.1 Determination of "As Likely to Happen As"

Using the same process described in Section 4.3.1.2, if the outcome of the qualitative assessment is sufficiently low, then the activity does not introduce any failures that are as likely to happen as those in the UFSAR. Therefore, the activity does not create a possibility for a malfunction of an SSC important to safety with a different result from any previously evaluated in the UFSAR.

If the outcome of the qualitative assessment is not sufficiently low, then the activity may introduce failures that are as likely to happen as those in the UFSAR that can create a possibility for a malfunction of an SSC important to safety with a different result from any previously evaluated in the UFSAR. For these cases, this evaluation criterion also needs to consider the impact of this potential failure on the safety analysis result using assumptions consistent with the facility's UFSAR.

4.3.6.2 Determination of Impact on Malfunction Result

For cases in which the qualitative assessment outcome is a failure likelihood of not sufficiently low, the impact on the result of a malfunction of an SSC important to safety needs to be assessed to determine if the result is different.

4.3.6.3 Types of Malfunctions

The key in evaluating the change is to determine the set of failures that are plausible at the appropriate level of detail, and whether they could disable the design function. A proposed activity that introduces a cross-tie or credible common mode failure (e.g., as a result of an analog to digital upgrade) should be evaluated further to see whether new outcomes have been introduced.

If a malfunction is not associated with a design function or a design bases function, then the malfunction cannot lead to dose to the general public. Unlike nuclear power reactors, design functions and design bases functions are not necessarily clearly identified in the UFSAR for a NPUF. Given that, there is a

benefit for reviewing the meaning of each. The three characteristics of design bases functions are summarized as follows:

1. Design bases functions are performed by SSCs that are required by, or otherwise necessary to comply with regulations, license conditions, orders, or tech specs, or credited in the safety analyses.

2. The functions of any individual SSC are functionally below that of design bases functions.

3. Design bases functions are derived primarily from the General Design Criteria.

For NPUFs, it is clear that the third characteristic does not apply. However, the design bases function can be proposed by the licensee by virtue of the content of the UFSAR Chapter 2, "Design Criteria." It should be noted that if an SSC can initiate an accident or transient, then it has a design function. Also, SSCs that support or impact design basis functions have (by definition) design functions.

The possible malfunctions with a different result are limited to those that are as likely to happen as those described in the UFSAR. For example, a seismic induced failure of a component that has been designed to the appropriate seismic criterion will not cause a malfunction with a different result. However, a proposed change or activity that increases the likelihood of a malfunction previously thought to be incredible, say from our example that the seismic induced failure of a component that has been designed to a lower seismic criterion to the point where it becomes as likely as the malfunctions assumed in the UFSAR could create a possible malfunction with a different result. Hence, for the purpose of the 10 CFR 50.59 evaluation, "credible" malfunctions are defined as those as likely as the malfunctions already assumed in the UFSAR.

4.3.6.4 Failure Analysis

In the power reactor community, it is common to evaluate malfunctions and their relationship with failure modes with what is called a Failure Modes and Effects Analysis. It is a formal step-by-step approach for identifying all possible failures in a design and the different consequences of those failures. It is an excellent approach for complex systems. This approach is likely overkill for most NPUFs due to the simplicity of design, low risk, and use of the MHA approach in accident analysis. A reasonable approach at an NPUF would simply be to examine the possible failure modes of the digital upgrade, how that is associated with a design function or design basis function, and consider whether the failure mode is applicable. It should be noted that it is up to the licensee to determine what is and what is not a design function or design basis function for their facility as they are rarely explicitly identified or defined in the UFSAR.

Results of the failure analysis should be used to identify the effects on the design function of failures that are as likely as those in the UFSAR. The effects of these failures should be compared to the failures addressed or assumed as part of the safety analyses in the UFSAR. If there is reasonable assurance that potential failures are not as likely as those described in the UFSAR, then such failures do not merit further consideration in the 10 CFR 50.59 evaluation.

For failures that are deemed as likely as the malfunctions in the UFSAR, the failure analysis performed during the design effort is used to "see whether new outcomes have been introduced." If the failure analysis shows that using only existing equipment and procedures, and with only minor procedural changes, there would be adequate backups to mitigate potential adverse impacts on design functions,

then for the purposes of the 10 CFR 50.59 evaluation, there would be no new outcome, and the change would be implemented under 10 CFR 50.59. The 10 CFR 50.59 evaluation would document the basis of this conclusion, along with any licensing commitments needed to ensure the future functionality of the backup.

Consideration of potential system failures and undesirable behaviors should be an integral part of the process of designing, specifying, and implementing a digital upgrade. Consideration of these undesirable events is referred to collectively as failure analysis. Failure analysis interacts with essentially all the main elements of the design process. It provides information needed to support evaluations, and it provides the context in which the digital upgrade issues ultimately can be resolved. Failure analysis examines what you do not want the system or device to do.

Failure analysis should not be a stand-alone activity, and it should not generate unnecessary effort or excessive documentation. It is part of the design process, and it can vary widely in scope depending on the extent and complexity of the upgrade. It should be performed as part of the process a facility has in evaluating a digital upgrade.

The purpose of the failure analysis is to ensure the system is designed with consideration of potential failures and undesirable behaviors such that the risk posed by these events is acceptable. Failure analysis should include the following elements, which are discussed in the subsequent sections:

- Identification of potential system-level failures 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 providing means for annunciating system failures to the operator.

One purpose of this evaluation of potential causes is to ensure that plausible system-level failure modes have been identified. Looking inside the system for potential failures can help identify system-level effects that may not have been obvious, particularly for a system with multiple inputs and outputs. In order to assess the likelihood of the system-level failures it is necessary to understand the potential causes and their likelihood of occurrence. However, this evaluation should go down only to a level in the design that is necessary to develop confidence that plausible system-level failure modes have been identified and that there is sufficient information to judge the likelihood of the system-level failures. Detailed component-level analyses without a focus on the system level can become overly burdensome, resulting in unnecessary effort and documentation, and can lose sight of the intent of the analysis. Hardware and software analyses may be taken to different levels of detail.

Evaluation of the causes of system failures should include consideration of:

- Hardware failures and software defects.

- Failures that may be caused by mis-operation of a human-system interface, either by operators or maintainers.

- Abnormal conditions and events including EMI-induced failures and other possible external events (e.g., loss of power, loss of environmental control, etc.).

- Failures that may be propagated to other systems through interconnections with external systems (e.g., digital communications).

This evaluation should include consideration of single, multiple, and possible common cause failures. In each case, the failure should be examined further to determine how and when it would be detected. Although directed toward nuclear power reactors, further information on performing and documenting failure analysis is provided in NRC RIS 2002-22, Supplement 1.

Example 4-18. Examining Failures at the System (Design Function) Level

Consider an instrument or device that monitors a single input signal and whose only UFSAR-described design function is to drive an output relay that serves as a trip input to a safety system. The safety system latches the trip signal when detected. It also drives a local indicator, but this is not part of a safety function and is not described in the UFSAR. The analog electronic instrument or device is to be replaced with a new, microprocessor-based instrument. It contains firmware which implements the simple trip logic based on the input signal and also provides processing to drive the local indicator. The new device performs exactly the same safety-related trip function as the previous device did, acting through a conventional relay.

Because the device has only a single output that is pertinent to its safety-related function (the relay contact), failures within the device would only affect the safety system through the behavior of the output relay. Therefore, identification of system-level failures is bounded by the failure modes of the output relay. In general, the failure modes of a relay contact output include:

- Fail open (inadvertent opening, failure of the contact in the open position, or failure of the contact to close on demand)

- Fail closed (inadvertent closing, failure of the contact in the closed position, or failure of the contact to open on demand)

- Fail intermittent (contact chatter, cycling, or random state changes).

In this example, assume the relay contact is normally closed and goes to the open position to initiate the trip function. Therefore, it could:

1. open spuriously, causing an unwanted trip of the system,

2. fail to open when needed (stick in the closed position), preventing a needed trip, or

3. cycle or chatter, in which case the effect is likely to be a spurious trip (the trip input signal is latched when it is sensed by the system).

These failure modes are bounded by what was considered previously for the analog unit: spurious trip or failure to trip. The licensee determines that although the new device employs a microprocessor and associated software to implement the safety-related function, there are no new failure modes at the system level and therefore no new effects or consequences other than what has been considered previously. This information will be used to support the 10 CFR 50.59 evaluation. (Note that the potential for increasing the likelihood of an already analyzed failure mode also must be considered by a separate evaluation question.)

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 facility that are important. Failures that impact 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 trips or transients that could challenge safety systems.

4.3.6.5 Resolution of Failures

While much of this discussion stems from the point of view of identifying failure modes or frequencies, it may be beneficial to identify or design aspects of redundancy and/or diversity to rectify the issue. Determining the appropriate resolutions for identified potential failures may include the following:

- No action – the failure does not pose significant risk and does not warrant any further consideration. This may be based on the assessment of likelihood of the failure, and a comparison to other contributors to risk. Engineering judgment is typically involved in making these assessments. Although rare, results of Probabilistic Risk Assessments (PRAs) may also help in this process and provide a context in which to judge the particular failure being considered among all the other acknowledged contributors to risk in the facility.

- 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. 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.

- 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.

For any potential failure that poses a significant risk, there should be a means to annunciate the failure to the operator, so the fault can be repaired promptly.

4.3.6.6 Software Common Cause Failures

Special consideration needs to be given to identifying software CCF. Qualitative Analysis results on the quality and design processes determine if there is reasonable assurance that the likelihood of failure due to software is sufficiently low. In this evaluation, "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 errors, calibration errors). Results of this evaluation are then used to determine whether failures due to software, including common cause failures, should be considered further in the 10 CFR 50.59 evaluation. If there is reasonable assurance that the likelihood of failure due to software is sufficiently low, then the upgrade would not require prior NRC review on the basis of software common cause failures.

Example 4-19. Transmitter Upgrade (NO CREATION of the Possibility for a Malfunction with a Different Result)

Proposed Activity

A large number of analog transmitters in several different systems and uses are being replaced with digital transmitters. These transmitters perform a variety of functions, including controlling the automatic actuation of devices (e.g., valve stroking) that are credited in a safety analysis. Engineering/technical information supporting the change showed that each digital transmitter was from a reputable manufacture, made under a quality control plan (although not a 10 CFR 50, Appendix B, QA plan), has a long history of operational use, have a very simple software architecture, has very few functions (one input and two outputs), and are easily tested.

Qualitative Assessment Outcome

A *qualitative assessment* was included in the engineering/technical information supporting the change. The *qualitative assessment* considered system design attributes, quality of the design processes employed, and operating experience of the proposed equipment. It was noted that utilizing this on many different systems within the facility may create the potential for a software CCF. However, due to the simplicity of the device and long operating history, it was concluded that the failure likelihood introduced by the modified SSCs is **sufficiently low**.

Conclusion

With the failure likelihood introduced by the modified SSCs being **sufficiently low**, the activity does not introduce any failures that are as likely to happen as those in the UFSAR that can initiate a malfunction of an SSC important to safety. Therefore, the activity does not create a possibility for a malfunction of an SSC important to safety with a different result from any previously evaluated in the UFSAR.

Example 4-20. Cooling System Control Upgrade (CREATION of the Possibility for a Malfunction with a Different Result)

Proposed Activity

A 250-kW research reactor proposes to replace all the various individual and independent analog control and monitoring systems for the cooling system with LabView® on a Windows® platform sending and receiving TTL signals to the various required digital transmitters/actuators. This would involve integrating the primary, secondary cooling pumps, flow rate sensors, and primary water level monitoring. Engineering/technical information supporting the change showed that the transmitter/actuators were from reputable manufactures, made under a quality control plan (although not a 10 CFR 50, Appendix B, QA plan), have a long history of operational use, have very simple architecture, and are easily tested. Engineering/technical information supporting the incorporation of the software packages showed that they were from reputable manufactures, made under a quality control plan (although not a 10 CFR 50, Appendix B, QA plan), and have a long history of operational use. However, the software architecture is considered complex for each package and they are not easily tested due to their complexity.

The USFAR-described design function of the primary and secondary cooling systems is to remove heat from the fuel and maintain the primary tank liner integrity (i.e., maintain less than a maximum primary tank temperature to prevent fatigue on joint welds leading to a loss of coolant). The UFSAR-described design function of the primary water level monitor is to alert the operator to a potential loss of coolant accident. Additionally, there technical specifications requiring operability and surveillance of the primary water level monitor.

Qualitative Assessment Outcome

A *qualitative assessment* was included in the engineering/technical information supporting the change. The *qualitative assessment* considered system design attributes, quality of the design processes employed, and operating experience of the proposed equipment. Due to the lack of simplicity and inability to thoroughly test each software package, let alone the combination of the two, it was concluded that the failure likelihood and potential software CCF introduced by the modified SSCs is **not sufficiently low**.

Conclusion

With the failure likelihood introduced by the modified SSCs being **not sufficiently low**, the activity does potentially introduce failures that are as likely to happen as those in the UFSAR that can initiate a malfunction of several SSCs important to safety. Therefore, the activity does create a possibility for a malfunction of an SSC important to safety with a different result from any previously evaluated in the UFSAR.

Example 4-21. Area Radiation Monitor Upgrade (NO CREATION of the Possibility for a Malfunction with a Different Result)

Proposed Activity

At an isotope production facility, there are 10 area radiation monitors (ARM) that monitor the environment for high radiation areas. These ARMs have a digital component and are obsolete. The facility wishes to replace them with a more current version of the same system. The replacement system

will also have similar digital components. All of the monitors will be from the same manufacturer and contain the same software. Engineering/technical information supporting the change showed that the newer system was from a reputable manufacture, made under a quality control plan (although not a 10 CFR 50, Appendix B, QA plan), has a long history of operational use, have a very simple software architecture, has very few functions (two inputs and two outputs), and are easily tested. Data from the manufacturer shows that the MTBF from the new system in comparison to the old system has increased from 10 years to 15 years.

The USFAR-described design function of the area monitoring system is not clear. There are no clear design functions or design basis functions identified in the USFAR that involve or credit the ARMs individually or as a system. However, there are technical specifications requiring operability and surveillance of a single ARM to be located in proximity to a reaction vessel. A provision exists in the technical specifications that allows for temporary monitoring to compensate for the loss of the required ARM until such a time when the ARM can be repaired or replaced. Therefore, the design function is based upon meeting the imposed technical specification requirement.

Qualitative Assessment Outcome

A *qualitative assessment* was included in the engineering/technical information supporting the change. The *qualitative assessment* considered system design attributes, quality of the design processes employed, and operating experience of the proposed equipment. It was noted that utilizing this on all ARM systems within the facility may create the potential for a software CCF. However, due to the simplicity of the devices, the long and proven operating history, and quality of manufacturing, it was concluded that the failure likelihood introduced by the modified SSCs is **sufficiently low**.

Conclusion

With the failure likelihood introduced by the modified SSCs being **sufficiently low**, the activity does not introduce any failures that are as likely to happen as those in the UFSAR that can initiate a malfunction of an SSC important to safety. Therefore, the activity does not create a possibility for a malfunction of an SSC important to safety with a different result from any previously evaluated in the UFSAR.

Example 4-22. Software Change (NO CREATION of the Possibility for a Malfunction with a Different Result)

Proposed Activity Description

A digital control system produces the control voltages for shim rod control stepper motors used by the operator to control the reactor. The regulating rod uses a separate faster fixed-speed DC motor. The maximum reactivity addition rate is credited in the safety analysis as an assumption when calculating peak power during a transient that ensures fuel safety limits are not exceeded. The assumption is that all control rods move at their maximum speed.

It is desired that the control voltage algorithm for automatic operation be adjusted to improve performance, slowing down the rod speed of stepper motor controllers to minimize power overshoot during power maneuvers. It is also desired to convert the DC-motor driven rod over to the same stepper

motor system. The software modification requires changes to several rod control files that affect rod speeds and the assigned stepper motors.

The software change quality control process controlled the requirements, specific changes, test plan and demonstrated that the affected changes could be thoroughly tested. However, an engineering evaluation determined the risk of failure of rod speed and other parts of the affected files could not be considered very low due to the complexity of the change, the new method of controlling the regulating rod, and the potential for programming errors. It was screened in for further evaluation.

An evaluation of the testing results demonstrated that no adverse effects were encountered, rods speeds were at the required values, and other functions controlled in the same file were not impacted. The evaluation concluded that the failure likelihood introduced by the modified SSCs was **sufficiently low.**

Evaluation Response

Two aspects are key to this example.

1. By adding the regulating rod to the stepper motor system the potential for common cause failure (software failure) is introduced to all the rods, not just the shim rods.

2. The rod speeds for the stepper motors are slower, including the regulating rod.

The activity does not create the possibility of a malfunction with a different result. The design function of controlling rod speed (overall reactivity addition rate) is maintained even with the introduction of the potential for a new malfunction. The system malfunction is bounded by what was previously evaluated in the UFSAR. Combined with the failure likelihood introduced by the modified SSCs being **sufficiently low**, the activity does not introduce any failures that are as likely to happen as those in the UFSAR that can initiate a malfunction of an SSC important to safety. Therefore, the activity does not create a possibility for a malfunction of an SSC important to safety with a different result from any previously evaluated in the UFSAR.

4.3.7 Does the Activity Result in a Design Basis Limit for a Fission Product Barrier Being Exceeded or Altered?

There is no unique guidance applicable to digital modifications for responding to this evaluation question because the identification of possible design basis limits for fission product barriers and the process for determination of "exceeded" or "altered" are not unique for a digital modification.

Fission product barriers include the fuel cladding, reactor coolant system boundary (e.g., the primary tank for most NPUFs) and containment, and the design basis limit pertains to the controlling numerical values in the UFSAR used to directly determine the integrity of such fission product barriers.

The first step in addressing this question is to determine if any of the numerical values used are associated with the change. If the design basis limit for the fission product barrier is controlled by another regulation specific to the parameter, then the effect on that limit is examined under the specific regulation. It would be unlikely that a design basis limit would be exceeded or altered as a result of a digital upgrade. However, the design basis limits could be affected if the timing (response time or processing time) of the digital device is different from that of the older analog system or if scaling

factors have been not implemented properly. For example, a primary digital display used by the operator to adhere to license power limits can affect the steady state flux levels, and thus assumptions in the thermal analysis could have the potential to be affected. The scope and results of testing should be carefully evaluated to ensure these potential errors are tested for and do not exist for critical parameters affecting design basis limits. If the change would result in the design basis limit for the parameter being exceeded, then the change would not be implemented under 10 CFR 50.59 and would require prior approval by the NRC. Similarly, if the change includes alteration of the numerical value of the design basis limit, NRC review would be required.

4.3.8 Does the Activity Result in a Departure from a Method of Evaluation Described in the UFSAR Used in Establishing the Design Bases or in the Safety Analyses?

There is no unique guidance applicable to digital modifications for responding to this evaluation criterion because activities involving methods of evaluation do not involve SSCs. This question applies to those analytical methods that are described in the UFSAR and demonstrate that the design meets the design bases or that the safety analysis is acceptable. A change to any element of the analysis methodology that produces a result that is not essentially the same as the prior analysis, or use of a method of evaluation not already approved by the NRC, constitutes a departure from a method of evaluation described in the UFSAR. Since licensees usually obtain NRC approval for changes to the analytical methods separately from implementing physical changes, either under 10 CFR 50.59 or via a license amendment request (LAR), it is unlikely that a digital upgrade would involve a departure from a method of evaluation.

5 REFERENCES

1. ASME NQA-1-1997, “Quality Assurance Requirements for Nuclear Facility Applications.”

2. ASME NQA-1 -2017 Subpart 2.7, “Quality Assurance Requirements for Computer Software for Nuclear Facility Applications.”

3. ASME NQA-2a-1990, “Quality Assurance Requirements for Nuclear Facility Applications.”

4. Code of Federal Regulations Title 10, Part 50.59, “Changes, Tests and Experiments.”

5. Code of Federal Regulations Title 10, Part 50.62, “Requirements for Reduction of Risk from Anticipated Transients Without Scram (ATWS) Events for Light-Water-Cooled Nuclear Power Plants.”

6. Code of Federal Regulations Title 10, Part 50, Appendix B, “Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants.”

7. EPRI NP-5652, “Guideline for the Utilization of Commercial Grade Items in Nuclear Safety Related Applications.”

8. EPRI TR-100516, “Nuclear Power Plant Equipment Qualification Reference Manual,” January 1992.

9. EPRI TR-102323, “Guidelines for Electromagnetic Interference Testing in Power Plants,” Revision 1, January 1997.

10. EPRI TR-102400, “Handbook for Electromagnetic Compatibility of Digital Equipment in Power Plants,” October 1994.

11. EPRI TR-103291, “Handbook for Verification and Validation of Digital Systems,” Revision 1, December 1998.

12. EPRI TR-104595, “Abnormal Conditions and Events for Instrumentation and Control Systems: Volume 1: Methodology for Nuclear Power Plant Digital Upgrades; Volume 2: Survey and Evaluation of Industry Practices,” January 1996.

13. EPRI TR-106439, “Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications,” October 1996.

14. EPRI TR-107339, “Evaluating Commercial Digital Equipment for High Integrity Applications: A Supplement to EPRI Report TR-106439,” December 1997.

15. EPRI TR-108831, “Requirements Engineering for Digital Upgrades,” December 1997.

16. EPRI TR-1001045, “Guideline on the Use of Pre-Qualified Digital Platforms for Safety and Non-Safety Applications in Nuclear Power Plants,” December 2000.

17. Federal Register Notice, “Changes, Tests, and Experiments,” Volume 64, Number 191, Pages 53582-53617, October 4, 1999.

18. Generic Letter 91-18, “Information to Licensees Regarding Two NRC Inspection Manual Sections on Resolution of Degraded and Non-Conforming Conditions and on Operability.”

19. IEC 60880, “Software for Computers in the Safety Systems of Nuclear Power Stations.”

20. IEC 61508, “Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems.”

21. IEEE 279-1971 (withdrawn), “Criteria for Protection Systems for Nuclear Power Generating Stations.”

22. IEEE 323-1983, “Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations.”

23. IEEE 338-1987, “Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems.”

24. IEEE 379-1994, “Standard Application of the Single Failure Criterion to Nuclear Power Generating Station Safety Systems.”

25. IEEE 603-1998, “Standard for Criteria for Safety Systems for Nuclear Power Generating Stations.”

26. ANSI/IEEE 730-1989, “IEEE Standard for Software Quality Assurance Plans.”

27. IEEE 828-1990, “IEEE Standard for Software Configuration Management Plans.”

28. IEEE 829-1983, “IEEE Standard for Software Test Documentation.”

29. IEEE 830-1993, “IEEE Recommended Practice for Software Requirements Specifications”

30. IEEE 1008-1987, “IEEE Standard for Software Unit Testing.”

31. IEEE 1012-1998, “Standard for Software Verification and Validation.”

32. ANSI/IEEE 1016, “IEEE Recommended Practice for Software Design Descriptions.”

33. IEEE 1042-1987, “IEEE Guide to Software Configuration Management.”

34. ANSI/IEEE 1063, “IEEE Standard for Software User Documentation.”

35. IEEE 1074-1995, “IEEE Standard for Developing Software Life Cycle Processes.”

36. IEEE 1228-1994, “Software Safety Plans.”

37. IEEE 7-4.3.2-1993, “Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations.”

38. ISA-RP67.04.01-2000, “Methodologies for the Determination of Setpoints for Nuclear Safety-Related Instrumentation.”

39. NEI 21-06, Revision 1, “Guidelines for 10 CFR 50.59 Implementation At Non-Power Production Or Utilization Facilities,” December 2021.

40. NEI White Paper, “Standard Format for Operating License Amendment Requests from Commercial Reactor Licensees,” March 15, 2001.

41. NSAC-105, “Guidelines for Design and Procedure Changes in Nuclear Power Plants.”

42. NUREG-0700, “Human-System Interface Design Review Guideline,” Revision 1, June 1996.

43. NUREG-0711, “Human Factors Engineering Program Review Model,” July 1994.

44. NUREG-0800, “Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants, Chapter 7,” Revision 4, June 1997.

45. NUREG-1709, “Selection of Sample Rate and Computer Word Length in Digital Instrumentation and Control Systems,” June 2000.

46. NUREG/CR-6294, “Design Factors for Safety-Critical Software,” October, 1994.

47. NUREG/CR-6303, “Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems,” December 1994.

48. Regulatory Guide 1.152, Revision 1, “Criteria for Digital Computers in Safety Systems of Nuclear Power Plants.”

49. Regulatory Guide 1.153, Revision 1, “Criteria for Safety Systems.”

50. Regulatory Guide 1.168, “Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants.”

51. Regulatory Guide 1.169, “Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants.”

52. Regulatory Guide 1.170, “Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants.”

53. Regulatory Guide 1.171, “Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants.”

54. Regulatory Guide 1.172, “Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants.”

55. Regulatory Guide 1.173, “Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants.”

56. Regulatory Guide 1.174, “An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis.”

57. Regulatory Guide 1.176, “An Approach for Plant-Specific Risk-Informed Decision making: Graded Quality Assurance.”

58. Regulatory Guide 1.180, “Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems.”

59. Regulatory Guide 1.187, “Guidance for Implementation of 10 CFR 50.59, Changes, Tests, and Experiments.”

60. Regulatory Guide 1.22, “Periodic Testing of Protection System Actuation Functions.”

61. draft Regulatory Guide DG-1077, “Guidelines for Environmental Qualification of Microprocessor-Based Equipment Important to Safety in Nuclear Power Plants.”

62. Regulatory Issue Summary 2022-22, Supplement 1, Clarification on Endorsement of the Nuclear Energy Institute Guidance in Designing Digital Upgrades in Instrumentation and Control Systems.

63. SECY-91-292, “Digital Computer Systems for Advanced LWR.”

64. Staff Requirements Memorandum, “SECY-93-087 – Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs,” July 21, 1993.

APPENDIX A. SUPPLEMENTAL GUIDANCE ON USE OF DIGITAL COMPONENTS AND SOFTWARE IN REACTOR SAFETY SYSTEMS

Unlike power reactors, NPUFs do not have a variety of guidance on the use of software or digital components for safety channels or ESFAS. As previously mentioned, use of Qualitative Assessments is not appropriate as they do not provide the level of detail or rigor that is needed for these important safety systems. As such, this appendix provides information pointing out which standards and guidance documents are in use in nuclear power plants, lacking specifics for NPUFs, for developing, designing, or incorporating digital components. This appendix is not intended to be comprehensive nor a step-by-step recipe. It is provided separately as an appendix because the level of quality, rigor, and expertise required to meet the expectations of determining the appropriateness of making a digital modification under 10 CFR 50.59 to reactor safety systems needs to be emphasized. For the purpose of this guidance, safety channels and ESFAS are consistent with the definition of "Reactor Safety Systems" found in ANSI/ANS 15.1, "The Development of Technical Specifications for Research Reactors."

The only guidance currently available specific for NPUFs is the Interim Staff Guidance Augmenting Chapter 7 of NUREG-1537. For reactor safety systems, that guidance points to IEEE 7-4.3.2-2010, "IEEE Standard Criteria for Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations." IEEE 7-4.3.2-2010 provides guidance on important elements of the development process. NUREG-1537 also recommends the use of ANSI/ANS 10.4-2008, "Verification and Validation of Non-Safety-Related Scientific and Engineering Computer Programs for the Nuclear Industry." Making changes to reactor safety systems under 10 CFR 50.59 should follow these standards. Note that this does not mean that these changes are required to meet the criteria for Class 1E systems as described in IEEE 308-2020, "IEEE Standard Criteria for Class 1E Power Systems for Nuclear Power Generating Stations."

The design of digital upgrades of these systems should place a high importance on quality and dependability. 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.

There are ample guidance documents that deal with the development of software and digital components of hardware. For applications where software or digital components are developed independently (i.e., not commercially purchased), either by the facility or by a contractor supporting an NPUF, it is recommended that one review Section 5, "Additional Guidance on Addressing Digital Upgrade Issues," of NEI 01-01, Rev. 1. However, caution should be used when implementing nuclear power plant guidance for NPUFs.