NRC Comments on NEI 96-07, Appendix D

On July 16, 2018, the Nuclear Energy Institute (NEI) submitted to the U.S. Nuclear Regulatory Commission (NRC), NEI 96-07, Appendix D, Revision 0f (ADAMS Accession No. ML18199A647). The enclosure to this cover page documents the NRC staff's comments (in comment bubbles) on this latest version of NEI 96-07, Appendix D. This document will be used to support a Category 2 public meeting with NEI to discuss these comments on August 30, 2018.

The NRC comments in this document are generally identified in two categories:

1. **Correction**:
   (a) Comment discussed at the June 26, Category 2 public meeting with NEI. Documentation of the meeting can be found in ADAMS under Accession No. ML18234A534. It is essential that these comments be addressed since, as written, they would result in situations of licensing uncertainty for both the licensees and inspectors.
   (b) Comments that document instances in the guidance where there exists a potential incorrect interpretation of referenced guidance (e.g., NEI 96-07 or RIS 2002-22) or regulation (such as 10 CFR 50.59). It is essential that these comments be addressed since, as written, they would result in situations of licensing uncertainty for both the licensees and inspectors.
2. **Enhancement** – Comments that document potential points of uncertainty and could be clarified.

General Appendix D Comments:

1. As written, there is an insufficient level of incorporation of RIS 2002-22, Supplement 1 guidance in Appendix D to say that the Supplement and/or NEI 01-01 could be superseded by Appendix D.

2. The examples in Appendix D, as written, are not complete enough to guide a licensee in making its determination on screening. The example conclusions should not be written in the context of "screens out" but rather "does not screen in" for the aspect or topic within the section/subsection. This approach should be applied to all examples. Because this document is used in conjunction with NEI 96-07, one can never reach a conclusion of "screens out" or "does not need a license amendment" but can only reach conclusions of "does not screen in for this aspect" or "does not require a license amendment request for this aspect." For example, use of malfunction results as the basis of conclusions for the examples is not appropriate because malfunction results are not the only consideration; whether the change introduces a new malfunction is only one consideration. Yet, the examples in Appendix D use this as the sole basis for conclusion.

3. Prior to the issuance of the qualitative assessment guidance from RIS 2002-22, Supplement 1, the definition of "engineering evaluations" was universally understood to mean "engineering/technical information supporting the change." However, since the

issuance of RIS 2002-22, Supplement 1 information, it is not clear from the NEI 96-07 draft whether “engineering evaluations” means “engineering/technical information supporting the change” or “qualitative assessment” This same comment is consistent for use of terms “qualitative assessment” and “technical assessment.”

4. Screening issues related to human-machine interface need to be resolved by a revision to Regulatory Guide 1.187 or a revision to NEI 96.07 rather than Appendix D. Human-machine interface issues are not unique to digital I & C and should be addressed in the broader context of the RG 1.187 or NEI 96.07.

5. The evaluation section of Appendix D appears to introduce new expansions of or paraphrasing of general 10 CFR 50.59 guidance without a clear nexus or explanation on why this is necessary for digital-specific modification. Specifically, section 4.3.6 Discussion of "different result" are not specific to digital I & C and should be worked, if needed, as a revision to the RG 1.187/NEI 96-07 documents and not in an appendix with limited applicability. Most of this area of concern may be addressed by the qualitative assessment approach documented in RIS 2002-22, Supplement 1.

NEI 96-07, Appendix D
Draft Revision 0f

Nuclear Energy Institute

SUPPLEMENTAL GUIDANCE FOR APPLICATION OF 10 CFR 50.59 TO DIGITAL MODIFICATIONS

July 2018

ACKNOWLEDGMENTS

NEI would like to thank the NEI 01-01 Focus Team for developing this document. Although everyone contributed to the development of this document, NEI would like to give special recognition to David Ramendick, who was instrumental in preparing this document.

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 96-07, Appendix D, *Supplemental Guidance for Application of 10 CFR 50.59 to Digital Modifications*, provides focused application of the 10 CFR 50.59 guidance contained in NEI 96-07, Revision 1, 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 appendix supersedes the 10 CFR 50.59-related guidance contained in NEI 01-01/ EPRI TR-102348, Guideline on Licensing of Digital Upgrades.

Commented [A1]: **Correction (a):** Currently, there is an insufficient level of incorporation of Supplement 1 to RIS 2002-22 guidance into Appendix D to say that NEI 01-01 and Supplement 1 could be superseded by Appendix D. See below for more detailed comments.

TABLE OF CONTENTS

EXECUTIVE SUMMARY i

1 INTRODUCTION 2

1.1 BACKGROUND 2

1.2 PURPOSE 3

1.3 10 CFR 50.59 PROCESS SUMMARY 3

1.4 APPLICABILITY TO 10 CFR 72.48 3

1.5 CONTENT OF THIS GUIDANCE DOCUMENT 3

2 DEFENSE IN DEPTH DESIGN PHILOSOPHY AND 10 CFR 50.59 3

3 DEFINITIONS AND APPLICABILITY OF TERMS 4

4 IMPLEMENTATION GUIDANCE 5

4.1 APPLICABILITY 5

4.2 SCREENING 5

4.3 EVALUATION PROCESS 24

5.0 EXAMPLES 62

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 Appendix was aligned with NEI 96-07, Rev. 1 text for ease of use. As such, there will be sections where no additional guidance is provided.

1.1 BACKGROUND

Commented [A2]: Correction (a): This section should include a summary of Supplement 1 to RIS 2002-22. This version and subsequent versions of Appendix D will use the guidance of Supplement 1 as a basis for guidance in this document. This is essential if NEI intends to eventually supersede NEI 01-01 and its supplement.

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. There also is great incentive to take advantage of modern digital technologies which 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 concern 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 as an issue and stated that NEI could separate technical guidance from 10 CFR 50.59 related guidance.

1.2 Purpose

Appendix D is intended to assist 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 appendix does not include guidance regarding design requirements for digital activities.

Commented [A3]: Enhancement: Recommend inserting here or on Section 1.5 below to add clarity for use:
"NEI 96-07, Appendix D, Supplemental Guidance for Application of 10 CFR 50.59 to Digital Modifications, does not alter, and unless explicitly noted, should not be interpreted differently than the guidance contained in NEI 96-07, Revision 1. Rather, Appendix D provides focused guidance for the application of the 10 CFR 50.59 to activities involving digital modifications."

Commented [A4]: Enhancement: Recommend inserting here or in Section 1.5 below to add clarity for use:
"While this appendix does not include guidance regarding design requirements for digital activities,
as with other plant modifications, fundamental to digital modifications is proper handling of key technical issues during the design process before 10 CFR 50.59 is applied. Appendix D describes three general types of failures that are specific to digital equipment (e.g., software related, other failure not software related, and human-system interface related) and the effects of these failures on the function of the system in which they are installed. The 10 CFR 50.59 process considers effects of a design change on a UFSAR-described design function 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 in paragraph 50.59(c)(2). In each section, Appendix D refers to specified 10 CFR 50.59 guidance in NEI 96-07, Revision 1, and then provides guidance for applying NEI 96-07 as-written to address the effects on the design function of these general types of failures that are specific to digital equipment."

The guidance in this appendix 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 be 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

No additional guidance is provided.

1.4 Applicability To 10 CFR 72.48

No additional guidance is provided.

1.5 Content Of This Guidance Document

No additional guidance is provided.

2 DEFENSE IN DEPTH DESIGN PHILOSOPHY AND 10 CFR 50.59

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 96-07, Rev. 1. Definitions specific to this appendix are defined below.

3.15 Sufficiently Low

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).

4 IMPLEMENTATION GUIDANCE

4.1 APPLICABILITY

No additional guidance is provided.

4.2 SCREENING

CAUTION

The guidance contained in this appendix is intended to supplement the generic Screen guidance contained in the main body in NEI 96-07, Section 4.2. Namely, the generic Screen guidance provided in the main body of NEI 96-07 and the more-focused Screen guidance in this appendix BOTH apply to digital modifications.

Commented [A5]: Correction (b): As written the staff is not clear on the intent of the second sentence of the Caution statement. Replace second sentence of the above CAUTION with:
"Unless specifically stated, the Screen guidance in this appendix does not alter and should not be interpreted differently than the generic Screen guidance provided in the main body of NEI 96-07. Rather, this appendix provides focused guidance for applying the guidance in the main body of NEI 96-07 to address the three general types of failures that are specific to digital equipment (e.g., software related, other failures not software related, and human-system interface related)."

Introduction

Throughout this section, references to the main body of NEI 96-07, Rev. 1 will be identified as "NEI 96-07."

As stated in NEI 96-07, 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 96-07 will be supplemented with the digital-specific guidance in the topic areas identified below.

Digital-to-Digital Replacements and "Equivalency"

In NEI 96-07, 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 time, 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 Appendix.

Guidance Focus

In the following sections and sub-sections that provide the Screen guidance unique to the application of 10 CFR 50.59 to digital modifications, each section and sub-section addresses only a specific aspect, sometimes ***at the deliberate exclusion of other related aspects***.

This focused approach is intended to concentrate on the particular aspect of interest and does not imply that the other aspects do not apply or could not be related to the aspect being addressed. Initially, all aspects need to be considered, with the knowledge that some of them may be able to be excluded based on the actual scope of the digital modification being reviewed.

Example Focus

Within this appendix, examples are provided to illustrate the guidance. Unless stated otherwise, a given example only addresses the aspect or topic within the section/sub-section in which it is included, sometimes ***at the deliberate exclusion of other aspects or topics*** which, if considered, could potentially change the Screen conclusion.

Human-System Interface Evaluations

Similar to other technical evaluations (performed as part of the design modification package), 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).

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

Introduction

A 10 CFR 50.59 Evaluation is required for digital modifications that adversely affect design functions, or the methods used to perform or control design functions. 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.

Commented [A6]: Correction (a) - Since the examples do not address all aspects, the conclusion should not be "screens out" but rather "does not screen in" for the aspect or topic within the section/subsection. This approach should be applied to all examples. That is, since this document is used in conjunction with NEI 96-07, one can never reach a conclusion of "screens out" or "does not need a license amendment" but can only reach conclusions of "does not screen in for this aspect" or "does not require a LAR for this aspect."

For NEI consideration:
(1) make it clear that the example only has one consideration that has been analyzed prior to documenting the conclusion, or.
(2) make the guidance examples reflect all considerations prior to documenting a conclusion

Commented [A7]: Correction (b): NEI 96-07 does not contain this statement and this approach is inconsistent with NEI 96-07 and could lead to confusion for both licensees and inspectors in implementation.

Enhancement: In NEI 96-07, **all** formal "Examples" (i.e., labeled "Example 1, Example 2) reach a final decision for screening and evaluation (e.g., Screens In OR Screens Out; 50.59 criterion Met OR 50.59 Criterion not Met). Otherwise, NEI 96-07 describes a specific aspect or topic within the guidance that precedes the formal "Example 1". To illustrate:

NEI 96-07 Section 4.1.6 states "Certain malfunctions are not explicitly described in the UFSAR because their effects are bounded by other malfunctions that are described. For example, failure of a lube oil pump to supply oil to a component may not be explicitly described because a failure of the supplied component to operate was described."

Please delete the example focus section for the reasons noted above. After addressing general comment 3, this section will no longer be necessary.

Commented [A8]: Correction (a) – deletion of this subsection as a global comment as indicated in NRC cover page.

- Replacement of hard controls (i.e., 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*.

Scope of Digital Modifications

Generally, a digital modification may consist of three areas of activities: (1) software-related activities, (2) hardware-related activities and (3) Human-System Interface-related activities.

NEI 96-07, 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.

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

SCOPE

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

(a) Use of Software and Digital Devices

(b) Combination of Components/Systems and/or Functions

USE OF SOFTWARE AND DIGITAL DEVICES

In NEI 96-07, Section 4.2.1, sub-section titled "Screening for Adverse Effects," the second paragraph contains the following guidance:

> "*...changes that would introduce a new type of accident or malfunction would screen in.*" [emphasis added]

Commented [A9]: **Enhancement:** Since both subsections (a) and (b) use the criteria of a new accident or malfunction, this text should be discussed within the scope section above.

Commented [A10]: **Correction (a):** Use of malfunction results should not be the only consideration for the basis of conclusions for determining an adverse impact in the examples.

Whether the change introduces a new malfunction is one consideration. Yet the examples use this as the only basis for conclusion.

Note that this Screen guidance does NOT address the "result(s)" of a new malfunction, which is the subject of Evaluation criterion (c)(2)(vi).

For applications involving SSCs with design functions, digital modifications that introduce the exact same software into redundant trains or channels to perform a design function have the potential to create a new malfunction. The potential to create a new malfunction comes from the possibility of a software CCF that did not previously exist.

For relatively simple digital modifications, engineering evaluations 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 the reliability of performing design functions is not decreased and no new malfunctions are created.

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 such as the following:

- Physical Characteristics of the Digital Modification
  - The change has a limited scope (e.g., replace analog transmitter with a digital transmitter that drives an existing instrument loop)
  - Uses a relatively simple digital architecture internally (simple process of acquiring one input signal, setting one output, and performing some simple diagnostic checks)
  - Has limited functionality (e.g., transmitters used to drive signals for parameters monitored)
  - Can be comprehensively tested (but not necessarily 100 percent of all combinations)
- Engineering Evaluation Assessments
  - 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 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

Commented [A11]: Correction (b): Change "The" to "One". This sentence states that "the" one way to introduce a new malfunction is from software CCF. It is very important to imply there may be other ways to introduce new malfunctions.

Commented [A12]: Correction (b): Reinsert the below guidance in that was deleted from the December 2017 version of Appendix D. This guidance is essential in that it addresses screening of software. Similar wording was also included in RIS 2002-22, Supplement 1.

"An adverse effect may also consist of the potential marginal increase in the likelihood of SSC 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 the redundant safety systems. On this basis, most digital modifications to redundant safety systems are adverse. However, for some digital modifications, engineering evaluations 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. Alternately, the use of different software in two or more redundant SSCs is not adverse due to a software common cause failure because there is no mechanism to increase in the likelihood of failure due to the introduction of software."

Reference May 2017 version of Appendix D, ADAMS Accession Number ML17137A020.

Commented [A13]: Correction (a): Prior to the issuance of the qualitative assessment guidance from RIS 2002-22, Supplement 1, the definition of "engineering evaluations" was universally understood to mean "engineering/technical information supporting the change." However, since the issuance of RIS 2002-22, Supplement 1 information, it is not clear from the NEI 96-07 draft whether "engineering evaluations" means "engineering/technical information supporting the change" or "qualitative assessment" Please change all uses of "engineering evaluations" to one of these options.

Commented [A14]: Correction (b): NRC has previously discussed this section with NEI and made suggested edits. Please change selected text to: "because software CCF is not introduced" to be consistent with previous discussion on this language.

Commented [A15]: Correction (b): Simplicity is not defined by the number of inputs and output – see example 4-1
Insert (e.g.) at the beginning of parenthesis.

- 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 illustrates the application of the guidance for a relatively simple digital modification.

Example 4-1. NO ADVERSE IMPACT on a Design Function for a Relatively Simple Digital Modification

Proposed Activity Description

Transmitters are used to drive signals for parameters monitored by redundant ESFAS channels. 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 Engineered Safety Features Actuation System (ESFAS) design function.

Design Function Identification

The ESFAS design function is the ability to respond to plant accidents.

Screen Response

The digital transmitters use a relatively simple digital architecture internally in that the firmware in the new transmitters implements a simple process of acquiring one input signal, setting one output, and performing some simple diagnostic checks.

Failures of the new digital device are encompassed by the failures of the existing analog device in that there are no new digital communications among devices that introduce possible new failure modes involving multiple devices. The engineering evaluation of the digital device 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 (one input and one output), it was comprehensively tested. Further, substantial operating history has demonstrated high reliability in applications similar to the ESFAS application.

Therefore, the proposed digital modification is *not adverse* because the digital modification is relatively simple and the assessment of the considerations

Commented [A16]: Correction (a): This example is implicitly providing guidance that simplicity is a function of the number or inputs and outputs, which is only part of the guidance above.

Simplicity is not defined by, or implied by, the number of inputs and outputs.

Deleting the entire "in that…" clause would resolve this concern.

Commented [A17]: Correction (a): Please delete.

The inclusion of "in that" creates a logical flaw. There are other ways to create new failure modes besides just digital communications.

Commented [A18]: Correction (a): This example is implicitly providing guidance that simplicity is a function of the number or inputs and outputs, which is only part of the guidance above.

Simplicity is not defined by the number of inputs and outputs.

Deleting the parenthetical clause would resolve this part of the concern.

identified above has determined that the reliability of performing the design function is not reduced and no new malfunctions are created.

Examples 4-2 and 4-3 illustrate the application of the *Use of Software and Digital Devices* aspect.

Example 4-2. NO ADVERSE IMPACT on a Design Function related to use of Software and Digital Devices

Proposed Activity Description

Two non-safety-related trains of main feedwater heaters exist, one for each train of main feedwater. Each main feedwater train consists of six feedwater heaters, for a total of 12 heaters. Each heater possesses an analog controller to control the water level in each of the heaters. Each analog controller is physically and functionally the same.

Each of the analog controllers will be replaced with its own digital controller. The hardware platform for each digital controller is from the same supplier and the software in each digital controller is exactly the same.

Design Function Identification

There are NO design functions associated with the feedwater heater water level controllers. The only UFSAR description related to the heaters states that the feedwater heater water level controllers are used to adjust the water levels in the heaters to optimize the thermal efficiency of the facility.

Screen Response

Since there are no design functions associated with the feedwater heater water level controllers, there are *no adverse* impacts.

Example 4-3. ADVERSE IMPACT on a Design Function related to use of Software and Digital Devices

Proposed Activity Description

Two non-safety-related main feedwater pumps (MFWPs) exist. There are two analog control systems (one per MFWP) that are physically and functionally the same.

The two analog control systems will be replaced with two 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.

Commented [A19]: **Correction (a):** NEI 96-07 States: "Design functions are UFSAR-described design bases functions and other SSC functions described in the UFSAR that support or impact design bases functions. Implicitly included within the meaning of design function are the conditions under which intended functions are required to be performed, such as equipment response times, process conditions, equipment qualification and single failure."

Feedwater, at the right temperature (i.e., heated) is a design function. Heater level control, or lack thereof can adversely affect the feedwater design function. Please clarify why feedwater heaters do not provide "NO design functions associated…"

Commented [A20]: **Correction (a):** This sentence implies that only explicit descriptions are considered, which is inconsistent with NEI 96-07, which states design function include "SSC functions described in the UFSAR that support or impact design bases functions." As stated in the example, the level controls are described in the UFSAR, and they support the feedwater function.

Design Function Identification

The design function of the feedwater control systems is to automatically control and regulate feedwater flow to the steam generators.

The UFSAR identifies the following MFWP control system malfunctions:

(a) failures causing the loss of one MFWP and its associated flow to the steam generators, and

(b) failures causing an increase in main feedwater flow to the maximum output from one MFWP.

Screen Response

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. There is an *adverse* impact on the design function of the main feedwater control system because the use of the exact same software in both digital control systems creates a new malfunction that could impact both MFWPs due to a potential software CCF.

Commented [A21]: Correction (a): This reasoning seems inconsistent with Example 4-4 below.

COMBINATION OF COMPONENTS/SYSTEMS AND/OR FUNCTIONS

Commented [A22]: Enhancement: Include more examples to illustrate the combinations of different system functions besides feedwater. Currently, having one example of different system combinations appears insufficient given challenges industry has expressed in screenings for complex 50.59 digital modifications.

The UFSAR may identify the number of components/systems, how the components/systems were arranged, and/or how functions, i.e., design requirements, were 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 the performance of *design functions*.

The combination of previously separate components/systems and/or functions, in and of itself, does not make the Screen conclusion adverse. Only if combining the previously separate components/systems and/or functions causes an adverse impact on a *design function* does the combination aspect of the digital modification screen in.

Commented [A23]: Correction (b): Delete “Only” and “does.” As stated previously by NEI, these sections and examples only address particular aspects; therefore, these words are inappropriate.

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*.

Examples 4-4 through 4-6 illustrate the application of the *Combination of Components/Systems and/or Functions* aspect.

Example 4-4. Combining Components and Functions with NO ADVERSE IMPACT on a Design Function

<u>Proposed Activity Description</u>

Two non-safety-related main feedwater pumps (MFWPs) exist. There are two analog control systems (one per MFWP) that are physically and functionally the same. Each analog control system has many subcomponents.

Option #1: Within each 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 components in each analog control system will be replaced with a separate digital control system.

Option #2: Instead of two separate, discreet, unconnected digital control systems being used for the feedwater control systems, only one central digital device is proposed to be used that will combine the previously separate control systems and control both main feedwater pumps.

<u>Design Function Identification</u>

Although the control systems and the major components are described in the UFSAR, only a design function for the feedwater control systems is identified. The design function of the feedwater control systems is to automatically control and regulate feedwater flow to the steam generators.

The UFSAR identifies the following MFWP control system malfunctions:

(a) failures causing the loss of <u>all</u> feedwater to the steam generators, and

(b) failures causing an increase in main feedwater flow to the maximum output from <u>both</u> MFWPs.

<u>Screen Response</u>

NOTE: Since the intent of this example is to illustrate the combination aspect ONLY, the software and hardware aspects will not be addressed in this example.

Option #1: There is *no adverse* impact on the design function of the main feedwater control systems to automatically control and regulate feedwater to the steam generators due to the combination of components in each of the two channels because no new malfunctions are created (i.e., the current malfunctions already consider the effect on both MFWPs).

Option #2: Although both main feedwater pumps would be affected by the failure of the one central digital processor, the proposed activity is *not adverse* because no new malfunctions are created (i.e., the current malfunctions already consider the effect on both MFWPs).

Commented [A24]: Correction (a): The parenthetical statement is incorrect. The statement is tying the combination to CCF. This reasoning is confused. The combination is within a channel, but the reasoning is about the impact on both channels, and this aspect of reasoning conflicts with example 4-3 above. In short the reasoning is "the failure is bounded by some other failure, therefore it is not a new failure, which is incorrect.

Each example in each section is only supposed to address one topic.

Suggested correction: (i.e., the current malfunctions already consider the effect on <u>each</u> MFWPs).

Commented [A25]: Correction (a):

(1)A new failure mode is created, and this should screen in, but this example reasoned that this new failure mode is bounded by a different failure mode, therefore it screens out. The effect of this guidance is to move "evaluation type activities" into the screening portion of the 50.59 process, which is inconsistent with the intent of NEI 96-07.

(2) But there is a reduction in independence which needs to be described. Previously the probability of both trains failing may have assumed the failures were independent, now the failures of both trains are dependent, this has the potential to reduce reliability which needs to be evaluated.

(3) There may also be a more than minimal increase of an accident since another way to create it has been found; therefore, it should be adverse for another reason.

NOTE: For both options, if the malfunctions had considered the effect on only one MFWP, the Screen conclusions would have been *adverse* because a new malfunction would have been created.

Example 4-5. Combining Components and Functions with NO ADVERSE IMPACT on a Design Function

Proposed Activity Description

A temperature monitor/controller in a room 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.

Design Function Identification

The temperature monitor/controller performs a design function to continuously monitor the temperature in the room to ensure the initial conditions are met should the emergency room coolers be needed.

The air damper controller performs a design function to continuously provide the appropriate air flow to the room to ensure the initial conditions are met should the emergency room coolers be needed.

There is no lower limit on the acceptable temperature in the room.

Screen Response

An engineering evaluation has documented the following malfunctions of the analog devices:

(1) failure of the temperature monitor/controller, causing the loss of input to the air damper controller and the ability of the air damper controller to control the temperature in the room, and

(2) failure of the air damper controller, causing the loss of the ability to control the temperature in the room.

Also documented in the engineering evaluation is the malfunction of the digital device, causing the loss of input to the air damper controller and the ability of the air damper controller to control the temperature in the room.

A comparison of the analog component and digital device malfunctions shows them to be the same. Therefore, although using the digital device might cause multiple design functions to not be performed, no new malfunctions are created. With no new malfunctions being created, there is *no adverse* impact on the design functions due to the combination aspect. Also, there are no indirect impacts that could affect the performance of the design functions due to the combination aspect.

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

Example 4-6 illustrates the combining of control systems from different, originally separate systems.

Example 4-6. Combining Systems and Functions with an ADVERSE IMPACT on a Design Function

Proposed Activity Description

Two non-safety-related analog feedwater control systems and one separate non-safety-related main turbine steam inlet valves analog control system exist.

All three analog control systems will be replaced with one digital control system that will combine the two feedwater control systems and the main turbine steam-inlet valve control system into a single digital device.

Design Function Identification

The design function of the feedwater control systems is to automatically control and regulate feedwater flow to the steam generators.

The design function of the main turbine inlet valve control system is to automatically control and regulate steam flow to the main turbine.

A review of the accident analyses identifies that none of the analyses consider the simultaneous failure of the feedwater control system and the failure of the main turbine control system.

Screen Response

Because new malfunctions have been introduced, there are *adverse* impacts on the design function of the main feedwater control systems and the design function of the main turbine control system due to the combination of components and functions from the three control systems.

Commented [A26]: **Correction (a):** This example implies guidance that is not provided explicitly above. Furthermore, the potential guidance that a reader might abstracted from this example is: even if multiple devices were postulated to fail independently, their concurrent failure (due to a change) is not a new malfunction. While in some cases this may be true, it is not true in all cases; however, no criteria are provided to distinguish between these two set of cases.

If there is any generally rule, it should be:
(1) "multiple malfunctions should screen in" or
(2) "multiple malfunctions is a new malfunction"

See general example comments mentioned above.

Delete the highlighted sentence or provide guidance in the subsection to connect to the highlighted sentence.

Commented [A27]: **Correction (a):** Another reason for it being adverse is that it is a reduction in independence.

See general example comment.

4.2.1.2 Screening of Changes to Procedures as Described in the UFSAR

Commented [A28]: Correction (a): NRC staff is recommending the deletion of this section from Appendix D (see general comments on HFE). However, should NEI wish to move forward with this section, the following comments will need to be resolved.

NEI should also consider the use of the terms HFE and HSI in this guidance document.

SCOPE

If the digital modification does not include or affect a Human-System Interface (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 96-07, 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 Human-System Interface (HSI), UFSARs will describe any 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.

There are three "basic HSI elements" of an HSI (Reference: 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, nuclear power plant personnel perform "four generic primary tasks" (Reference: NUREG/CR-6947):

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

Table 1 contains examples of modifications to each of the three basic HSI elements applicable to this Screen consideration.

Table 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 HSI (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 a 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 HSI assessment 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 negatively impacts an individual's ability to perform the generic primary task.

  Examples of negative impacts on an individual's performance that may 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.

After the two-step HSI assessment, the final step is application of the standard Screen assessment process (i.e., identification of design functions and determination of *adverse* or *not adverse*, including the justification for the conclusion).

<u>SIMPLE HUMAN-SYSTEM INTERFACE EXAMPLE</u>

Example 4-7 illustrates how a digital modification with HSI considerations would be addressed.

Example 4-7: Assessment of Modification with NO ADVERSE IMPACT on a UFSAR-Described Design Function

<u>Proposed Activity Description</u>

Currently, a knob is rotated clock-wise to open a flow control valve 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.

<u>HSI Assessment Process</u>

STEP 1. Identification of the Generic Primary Tasks Involved:

Commented [A29]: Enhancement: This process proposes a two-step HSI process and a third step (described below) for performing the screening task (i.e., determine whether a change is adverse). This step contains technical guidance regarding HSI evaluations (i.e., the two-step HSI assessment), but not guidance on how to convert the technical conclusion (i.e., there is a negative impact or not) into a screening evaluation (i.e., adverse or not).

Commented [A30]: Enhancement: No guidance is provided on how to do this step. Furthermore, probably only an HFE professional can do this adequately.

Commented [A31]: Correction (a): Delete "may" otherwise this guidance is saying "negative impacts" may or may not be adverse; no guidance is provided how to distinguish these two.

Please compare with Examples 4-8a & 4-8b below. In both of these examples, an HFE review determined the HFE modification to have a negative impact, but the 50.59 screening determined to be not adverse.

This guidance is inconsistent with NEI 96-07 Rev. 1 Section 4.2.1, subsection: "<u>Screening for Adverse Effects</u>" which states: "The screening process is not concerned with the magnitude of adverse effects that are identified. Any change that adversely affects ... is screened in. The magnitude of the adverse effect (e.g., is the minimal increase standard met?) is the focus of the 10 CFR 50.59 evaluation process."

Furthermore NEI 96-07 Section 4.2.1.2 states: "Proposed changes that are determined to have positive or no effect on how SSC design functions are performed or controlled may be screened out."

Commented [A32]: Enhancement: This is the third step.

Commented [A33]: Correction (a): Any increase should be understood as adverse and this should be stated in this paragraph.

Please compare with Examples 4-8a & 4-8b below. In both of these examples, an HFE review determined the HFE modification to have a negative impact, but the 50.59 screening determined to be not adverse. Appendix D, provides no guidance for determining how much of an increase or how many types of increases result in and adverse determination.

Please delete this clause. That is, the HFE professional determines whether there is a negative impact, and their 50.59 engineer determines whether a design function is affected.

(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:

As part of the technical evaluation supporting the proposed modification, a HFE evaluation was performed.

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

Task 4 was identified as involved; the HFE evaluation determined that the change from knob to touch screen would not have a negative impact because it does not affect the operator's ability to perform the response implementation task.

Identification and Assessment of the Relevant Design Function(s)

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 to allow the operator to manually adjust the position of the flow control valve and the UFSAR description implicitly identifies the SSC (i.e., the knob).

Using the results from the HFE evaluation and examining the replacement of the "knob" with a "touch screen," the modification is *not adverse* 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 the UFSAR-described design function.

COMPREHENSIVE HUMAN-SYSTEM INTERFACE EXAMPLES

Examples 4-8a and 4-8b illustrate how a digital modification with HSI considerations would be addressed.

Although both examples use the same basic digital modification, Example 4-8a illustrates a *no adverse* impact case and Example 4-8b illustrates an *adverse* impact case by "complicating" the HSI portion of the modification.

Example 4-8a. Digital Modification Involving HSI Considerations with NO ADVERSE IMPACT on a Design Function

Proposed Activity Description

Analog components and controls for a redundant safety-related system are to be replaced with digital components and controls, including new digital-based HSI.

Currently, two redundant channels/trains of information and controls are provided to the operators in the Main Control Room for the redundant systems. For each 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 redundant hard-wired switches, indicator lights and analog meters. The new HSI consolidates the information and controls onto two flat panel displays (one per train) with touch screen “soft” controls. The information available on the flat panels is equivalent to that provided on the current analog HSI. Each 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.

HSI Assessment Process

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:

As part of the technical evaluation supporting the proposed modification, a hsi evaluation was performed.

Task 1 is involved. Any change to information presentation has the potential to impact the operator's ability to monitor and detect changes in plant parameters. Even though the modification will result in information being presented on flat panels, the information available and the organization of that information (i.e., by train) will be equivalent to the existing HSI. Due to this equivalence and additional favorable factors (e.g., appropriate sized flat panels, appropriate display brightness, clearly identified function buttons, etc.) as documented in the HFE evaluation, there is no impact to 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). 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 negatively impacts the operator's ability to respond because the modification increases the difficulty of implementing a response by requiring four actions instead of one action and the additional actions result in an increase in the operator's time to respond.

Commented [A34]: Correction (a): Connected to previous comments.

Compare to conclusion below.

This example conflicts with NEI 96-07 by stating that a negative effect on a design function is not adverse and screens out.

Identification and Assessment of Design Functions

Design Function Identification

(a) Status indications are continuously available to the operator.

(b) The operator controls the system components manually.

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 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 on satisfaction of design function (b).

Commented [A35]: Correction (a): Compare to HFE evaluation above.

This example conflicts with NEI 96-07 by stating that a negative effect on a design function is not adverse and screens out.

Example 4-8b. Digital Modification Involving HSI Considerations with an ADVERSE IMPACT on a Design Function

Proposed Activity Description

Analog components and controls for a redundant safety-related system are to be replaced with digital components and controls, including new digital-based HSI.

Currently, two redundant channels/trains of information and controls are provided to the operators in the Main Control Room for the redundant systems. For each 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 redundant hard-wired switches, indicator lights and analog meters. The new HSI consolidates the information and controls onto two flat panel displays (one per train) with touch screen “soft” controls. The information available on the flat panels is equivalent to that provided on the current analog HSI. Each 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. Each flat panel display can be *customized* to display the parameters and/or the configuration (e.g. by train, 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.

HSI Assessment Process

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:

As part of the technical evaluation supporting the proposed modification, a HFE evaluation was performed.

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 negatively impacting their ability to monitor the plant and detect changes. In addition, altering the information displayed and the organization of the information will negatively impact the operator's understanding of how the information relates to system performance. This negative impact on understanding will also negatively impact the operator's ability to assess the situation and plan an appropriate response.

Commented [A36]: Correction (a): Compare with conclusion (a) below.

This example conflicts with NEI 96-07 by stating that a negative effect on a design function is not adverse and screens out.

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). 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 negatively impacts the operator's ability to respond because the modification increases the difficulty of implementing a response by requiring four actions instead of one action and the additional actions result in an increase in the operator's time to respond.

Commented [A37]: Correction (a): Compare with conclusion (b) below.

This example conflicts with NEI 96-07 by stating that a negative effect on a design function is not adverse and screens out.

<u>Identification and Assessment of Design Functions</u>

<u>Design Function Identification</u>

(a) Status indications are continuously available to the operator.

(b) The operator controls the system components manually.

<u>Screen Response</u>

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 on design function (a).

Commented [A38]: Correction (a): This conclusion only addresses one of the negative conclusions reached in the HFE evaluation; does this mean the others do not have an adverse effect? What guidance states what does or does not have an adverse effect?

This example conflicts with NEI 96-07 by stating that a negative effect on a design function is not adverse and screens out.

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 on satisfaction of design function (b).

Commented [A39]: Correction (a): Compare with HFE evaluation above.

This example conflicts with NEI 96-07 by stating that a negative effect on a design function is not adverse and screens out.

Since there is an adverse impact on design function (a), the overall conclusion of the Screen for this consideration would be *adverse*.

4.2.1.3 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, not a *method of evaluation* described in the UFSAR (see NEI 96-07, 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 in the facility. The response to this Screen consideration should reflect this distinction.

A necessary revision or replacement of a ***method of evaluation*** (see NEI 96-07, Section 3.10) resulting from a digital modification is separate from the digital modification itself and the guidance in NEI 96-07, Section 4.2.1.3 applies.

4.2.2 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, not a test or experiment (see NEI 96-07, Section 4.2.2). The response to this Screen consideration should reflect this characterization.

A necessary ***test or experiment*** (see NEI 96-07, Section 3.14) involving a digital modification is separate from the digital modification itself and the guidance in NEI 96-07, Section 4.2.2 applies.

4.3 EVALUATION PROCESS

CAUTION

The guidance contained in this appendix is intended to supplement the generic Evaluation guidance contained in the main body in NEI 96-07, Section 4.3. Namely, the generic Evaluation guidance provided in the main body of NEI 96-07 and the more-focused Evaluation guidance in this appendix BOTH apply to digital modifications.

Introduction

Throughout this section, references to the main body of NEI 96-07, Rev. 1 will be identified as "NEI 96-07."

Guidance Focus

In the following sections and sub-sections that describe the Evaluation guidance particularly useful for the application of 10 CFR 50.59 to digital modifications, each section and sub-section describes only a specific aspect, sometimes ***at the deliberate exclusion of other related aspects***. This focused approach is intended to concentrate on the particular aspect of interest and does not imply that the other aspects do not apply or could not be related to the aspect being addressed.

Example Focus

Examples are provided to illustrate the guidance provided herein. Unless stated otherwise, a given example only addresses the specific aspect or topic within the section/sub-section in which it is included, sometimes ***at the deliberate exclusion of other aspects or topics*** that, if considered, could potentially change the Evaluation conclusion.

Qualitative Assessment

For digital I&C systems, reasonable assurance of low likelihood of failure is derived from a qualitative assessment of factors involving the design attributes of the modified SSC, the quality of the design processes, and 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 and reasoning for making a determination that there is reasonable assurance that the digital I&C modification will exhibit a low likelihood of failure by considering the aggregate of these factors.

SSC Failure Likelihood Determination Outcomes

The possible outcomes of an engineering evaluation (e.g., qualitative assessment), performed in accordance with applicable Industry and/or NRC guidance documents, are as follows:

(1) SSC failure likelihood is **sufficiently low** (as defined in Definition 3.15), or

(2) SSC failure likelihood is **not sufficiently low**.

Commented [A40]: Correction (a): The evaluation section of Appendix D appears to introduce new expansions of or paraphrasing of general 10 CFR 50.59 guidance without a clear nexus or explanation on why this is necessary for digital-specific modification. Clarifications of general 50.59 guidance topics should be made within the main body of NEI 96-07. Appendix D should avoid unnecessary expansion of general 50.59 concepts already covered in the main body of NEI 96-07 unless specifically demonstrated to be uniquely necessary for digital modifications, as demonstrated by Section 4.2's screening guidance on combination of components/functions subsection. ***Proper incorporation of the guidance of Supplement 1 to RIS 2002-22 obviates the need for expansion, refinement or paraphrasing of general 50.59 concepts from the main body of NEI 96-07 revision 1 for evaluation guidance.***

Commented [A41]: Correction (a): Since a qualitative assessment is used to address more than one evaluation question, the guidance for performing it should be in one place, presumably in this sub-section.

Very little qualitative assessment guidance from Supplement 1 to RIS 2002-22 has been incorporated.

Furthermore, the restrictions on the applicability of the qualitative assessment have not been incorporated.

Commented [A42]: Correction (a): Supplement 1 to RIS 2002-22 defines a particular type of qualitative assessment germane to 50.59 evaluations, based upon the guidance of NEI 01-01. This paragraph appears to define the general concept of a qualitative assessment with that described in Supplement 1. This distinction should be made when introducing this concept here and made more clearly in subsequent discussion of a qualitative assessment, as described in the RIS supplement to be applied to evaluation criteria.

Commented [A43]: Correction (a): Little guidance from Supplement 1 to RIS 2002-22 has been incorporated. Specifically information from Section 2 of the RIS has been omitted.

If the SSC failure likelihood is determined to be **sufficiently low**, then by extension, the likelihood of software CCF is also considered to be **sufficiently low**.

If the failure likelihood of the modified SSC is not examined as part of an engineering evaluation, then the failure likelihood of the modified SSC will be assumed to be **not sufficiently low** for purposes of responding to the following 10 CFR 50.59 Evaluation criteria.

These possible outcomes (i.e., **sufficiently low** or **not sufficiently low**) will be used in developing the responses to Evaluation criteria 1, 2, 5 and 6.

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

Commented [A44]: Correction (b): This section contains many instances that are contrary to 50.59(c)(2)(i).

Neither the 50.59 regulation nor NEI 96-07, Section 4.3.1, use the word "initiator." Therefore

- only "an accident," **not** an "accident initiator" must be explicitly mentioned in the UFSAR., and
- a "more than minimal increase in the frequency of an accident, "as a result of the change could be for **any** reason such a new, entirely different initiator that was introduced by the change.

See specific comments below…

<u>INTRODUCTION</u>

From NEI 96-07, Section 3.2:

> "*The term 'accidents' refers to the anticipated (or abnormal) operational transients and postulated design basis accidents...*"

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

After applying the generic guidance in NEI 96-07, Section 4.3.1 to identify any accidents affected by the systems/components involved with the digital modification and examining the initiators of those accidents, the impact on the frequency of the initiator (and, hence, the accident itself) due to the digital modification can be assessed.

Commented [A45]: Correction (b): Contrary to 50.59 and NEI 96-07. As described in the above comment, an increase in frequency can be for **any** reason and is not limited by "examining the initiators of those accidents" because the change can introduce a new, entirely different initiators.

Commented [A46]: Enhancement: To address comments regarding "accident initiators," the NRC staff recommends wording from NEI 96-07, Section 4.3.1, which states, "In answering this question, the first step is to identify the accidents that have been evaluated in the UFSAR that are affected by the proposed activity. Then a determination should be made as to whether the frequency of these accidents occurring would be more than minimally increased".

Alternate recommended wording: NEI 01-01, Section 4.3.1,
"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"

All accident initiators 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 accident initiators 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, 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 accident frequency due to the digital system's compatibility with the environment in which the system is being installed, which would be addressed by applying the general guidance related to meeting applicable regulatory requirements and other acceptance criteria to which the licensee is committed, and departures from standards as outlined in the general design criteria, as discussed in NEI 96-07, Section 4.3.1 and Section 4.3.1, Example 2.

For a digital modification, the assessment for personnel-related sources will consider the impact due to the Human-System Interface (HSI).

Typically, numerical values quantifying an accident frequency are not available, so the qualitative approach using the *attributable* (i.e., causal relationship) and the *negligible/discernable* (i.e., magnitude) criteria from NEI 96-07, Section 4.3.1 will be examined in this guidance.

GUIDANCE

Determination of Attributable (i.e., Causality)

NOTE: This guidance is not unique to digital and is the same as that provided in NEI 96-07, Section 4.3.1. This guidance is included here for completeness.

If none of the components/systems involved with the digital modification are identified as affecting an accident initiator previously identified in the UFSAR, then there is no attributable impact on the frequency of occurrence of an accident.

Alternately, if any component/system involved with the digital modification is identified as affecting an accident initiator previously identified in the UFSAR, then an impact on the frequency of occurrence of an accident can be attributed to the digital modification. If an attributable impact is identified, then further assessment to determine the magnitude of the impact will be performed.

Examples 4-9 and 4-10 will illustrate the application of the *attributable* criterion.

Example 4-9 illustrates a case of NO *attributable* impact on the frequency of occurrence of an accident.

Example 4-9. NO ATTRIBUTABLE Impact on the Frequency of Occurrence of an Accident

Proposed Activity Description

Two safety-related containment chillers exist. There are two analog control systems (one per chiller) 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 the same supplier and the software in each digital control system is exactly the same.

Affected Accidents and Accident Initiators

The review of the UFSAR accident analyses identified the Loss of Coolant Accident (LOCA) and Main Steam Line Break (MSLB) events as containing requirements related to the safety-related containment chillers. Specifically, the UFSAR states the following: "To satisfy single failure requirements, the loss of only one control system and its worst-case effect on the containment post-accident [emphasis added] environment due to the loss of one chiller has been considered in the LOCA and MSLB analyses."

Therefore, the affected accidents are LOCA and MSLB.

The UFSAR identified an equipment-related initiator for both accidents as being a pipe break. For LOCA, the pipe break occurs in a hot leg or a cold leg. For MSLB, the pipe break occurs in the main steam line exiting the steam generator.

Impact on Accident Frequency

In these accidents, the safety-related containment chillers are not accident initiators (i.e., they are not pipe breaks). Furthermore, the chillers are only considered as part of accident mitigation; after the accidents have already occurred. Therefore, there is NO impact on the frequency of occurrence of the accidents that can be *attributed* to the digital modification.

Commented [A47]: Correction (a): This type of criteria may be applicable to "malfunctions"; however, what is applicable to question (i) (i.e., "accidents") is the AOOs or DBAs that the chiller failures and misbehaviors would create. This example appears to provide a methodology for determining whether a modification relates to an accident initiator. It is not clear why this method will always be conservative.

For example ESFAS mitigates against certain accidents. The ESFAS is not an initiator of those accidents that it mitigates. By the reasoning implied in this example, the ESFAS could not impact the frequency of an accident. However, a spurious ESFAS actuation is itself an accident.

It is not apparent that this example considers whether the failure of the components could be a different accident than one that it mitigates (i.e., the chillers do not contribute to the LOCA).

Commented [A48]: Correction (a): This example considers the outcomes of an event. Clarify the relevance of the outcome when determining the frequency of the event.

Example 4-10 illustrates a case of an *attributable* impact on the frequency of occurrence of an accident.

Example 4-10. ATTRIBUTABLE Impact on the Frequency of Occurrence of an Accident

Proposed Activity Description

Two non-safety-related main feedwater pumps (MFWPs) exist, each with its own flow control valve. There are two analog control systems (one per MFWP 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 the same supplier and the software in each digital control system is exactly the same.

Affected Accident and Accident Initiators

The affected accident is the Loss of Feedwater event. The UFSAR identifies the equipment-related initiators as being the loss of one MFWP or the closure of one MFWP flow control valve.

Impact on Accident Frequency

In this accident, the non-safety-related feedwater system is related to the accident initiators (i.e., loss of a MFWP and/or closure of a flow control valve). Therefore, an impact on the frequency of occurrence of the accident can be *attributed* to the digital modification. (NOTE: The magnitude of the impact would be assessed next.)

Determination of Negligible/Discernable (i.e., Magnitude)

NOTE: The guidance in this sub-section applies ONLY when an *attributable* impact on the frequency of occurrence of an accident has been established.

For proposed activities in which there is an *attributable* impact on the frequency of occurrence of an accident, the *negligible/discernable* portion of the criteria (i.e., magnitude) also needs to be assessed.

To determine the overall effect of the digital modification on the frequency of an accident, an engineering evaluation is performed. An engineering evaluation that uses a qualitative assessment to judge the failure likelihood of the modified SSC should consider each factor identified below:

Commented [A49]: Enhancement - Please explain the change from software CCF to failure likelihood.

This same comment applies to Section 4.3.2.

- Design attributes employed
- Quality of the design processes, and
- Operating experience of the software and hardware used (i.e., product maturity and in-service experience).

Negligible:

To achieve a *negligible* conclusion, the engineering evaluation of each factor (e.g., as documented in a qualitative assessment) would conclude that the affected SSC will exhibit a **sufficiently low** likelihood of failure, and by extension, that 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)**"*[1] [***emphasis*** added].

Commented [A50]: Correction (a): Conflicts with paragraph below. In short, this paragraph states that "sufficiently low" means that there is "no clear trend…"

Therefore, if the qualitative assessment outcome is **sufficiently low**, there is not more than a minimal increase in the frequency of occurrence of an accident previously evaluated in the UFSAR.

Discernable:

[1] Refer to NEI 96-07, Section 4.3.1, Example 1.

If the examination of each factor concludes that the change in the accident frequency exhibits a clear trend towards increasing the frequency, then a *discernable* increase in the accident frequency would exist. In this case, the software CCF likelihood could be **sufficiently low** or **not sufficiently low**.

The engineering evaluation (e.g., the qualitative assessment) is also used to determine if the *discernible* increase in the accident frequency is "more than minimal" or "NOT more than minimal." To achieve a conclusion of "NOT more than minimal," the proposed activity must 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.

Examples 4-11 and 4-12 illustrate the *negligible/discernable* portion (i.e., magnitude) of the criteria and assume the *attributable* portion of the criteria has been satisfied.

Example 4-11 illustrates a case with a *negligible* change to the accident frequency.

Example 4-11. NEGLIGIBLE Impact on the Frequency of Occurrence of an Accident

Proposed Activity Description

Two non-safety-related main feedwater pumps (MFWPs) exist, each with its own flow control valve. There are two analog control systems (one per MFWP 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 the same supplier and the software in each digital control system is exactly the same.

Magnitude Conclusion

A qualitative assessment performed as part of the design process, considering system design attributes, quality of the design processes employed, and operating experience of the proposed equipment, concluded that the failure likelihood of the modified SSC is **sufficiently low**.

Commented [A51]: Correction (a): Conflicts with paragraph above. In short, this paragraph states that "a clear trend towards increasing" means nothing with respect to "sufficiently low" of software CCF. The logic in transition between negligible and discernable is not clear when sufficiently low or not sufficiently low is determined,

Furthermore this paragraph seems to be inconsistent with the definition of sufficiently low in Section 3.15 of Appendix D.

This same comment applies to Section 4.3.2.

Commented [A52]: Correction (b): This criteria is necessary but not sufficient to demonstrate no more than a minimum increase. For example, if the accident frequency is doubled but the modification still meets requirements, the criteria would allow this change to be made under 50.59.

This is contrary to NEI 96-07, section 4.3.1. If the qualitative assessment determines that the propose mod is **not** sufficiently low, then meeting applicable requirement is not sufficient to say that it is not more than minimum increase.

This is applicable to the staff's review of Example 4-12.

All applicable requirements and other acceptance criteria to which the licensee is committed, as well as applicable design, material and construction standards, continue to be met.

Therefore, the change in the frequency of occurrence of the Loss of Feedwater event is *negligible* due to the effect of the factors considered in the qualitative assessment.

Overall Conclusion

Although an attributable impact on the frequency of occurrence of the Loss of Feedwater event was determined to exist, there was no clear trend toward increasing the frequency. With no clear trend toward increasing the frequency, there is not more than a minimal increase in the frequency of occurrence of the accident due to the digital modification.

Example 4-12 illustrates a case with a *discernable* increase to the accident frequency.

Example 4-12. DISCERNABLE Increase in the Frequency of Occurrence of an Accident

Proposed Activity Description

Same as Example 4-11.

Magnitude Conclusion

Based on the qualitative assessment performed as part of the technical assessment supporting this digital modification, the likelihood of failure causing the loss of both feedwater control systems (resulting in the loss of both MFWPs) has been determined to be **not sufficiently low**.

All applicable requirements and other acceptance criteria to which the licensee is committed, as well as applicable design, material and construction standards, continue to be met.

The change in the frequency of occurrence of the Loss of Feedwater event is *discernable* due to the effect of the factors considered in the qualitative evaluation.

Overall Conclusion

An attributable impact on the frequency of occurrence of the Loss of Feedwater event was determined to exist and there is a clear trend towards increasing the frequency. The clear trend toward increasing the frequency (i.e., the *discernable* increase) is due to the software CCF likelihood being **not sufficiently low**.

However, even with a clear trend towards increasing the frequency, the assessments and conclusions documented in the qualitative assessment of the considered factors and the satisfaction of applicable requirements and other acceptance criteria to which the licensee is committed, as well as applicable design, material and construction standards, there is NOT more than a minimal increase in the frequency of occurrence of the accident due to the digital modification.

Commented [A53]: Correction (a): Meeting applicable requirements and standards is necessary but not sufficient. See comment above.

HUMAN-SYSTEM INTERFACE ASSESSMENT

Commented [A54]: Enhancement: This section does not contain any digital unique guidance; therefore, it can be deleted. Same comment applies to Sections 4.3.1, 4.3.2, 4.3.5., and 4.3.6

If no personnel-based initiators involving degraded operator performance (e.g., operator error) are identified among the accident initiators, then an increase in the frequency of the accident cannot occur due to the Human-System Interface portion of the digital modification. Otherwise, the application of the *attributable* criterion (i.e., causality) and the *negligible/discernable* criterion (i.e., magnitude) are assessed utilizing the guidance described in NEI 96-07, Section 4.3.1.

Commented [A55]: Enhancement: There is almost no guidance related to attributable and negligible/discernable in NEI 96-07. Furthermore, is it necessary to say, once again, to follow the guidance in NEI 96-07?

This same comment applies to Sections 4.3.1, 4.3.2, 4.3.5., and 4.3.6.

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?

INTRODUCTION

After applying the generic guidance in NEI 96-07, Section 4.3.2 to identify any malfunctions affected by the systems/components involved with the digital modification and examining the initiators of those malfunctions, the impact on the likelihood of the initiator (and, hence, the malfunction itself) due to the digital modification can be assessed.

All malfunction initiators 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 malfunction initiators 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, which would be addressed by applying the general guidance related to meeting applicable regulatory requirements and other acceptance criteria to which the licensee is committed, and departures from standards as outlined in the general design criteria, as discussed in NEI 96-07, Section 4.3.2.

For a digital modification, the assessment for personnel-related sources will consider the impact due to the Human-System Interface (HSI).

Typically, numerical values quantifying a malfunction likelihood are not available, so the qualitative approach using the *attributable* (i.e., causal relationship) and the *negligible/discernable* (i.e., magnitude) criteria from NEI 96-07, Section 4.3.2 will be examined in this guidance.

GUIDANCE

Impact on Redundancy, Diversity, Separation or Independence

As discussed in NEI 96-07, Section 4.3.2, Example 6, a proposed activity that reduces redundancy, diversity, separation or independence is considered more than a minimal increase in the likelihood of a malfunction and requires prior NRC approval. However, licensees may reduce excess redundancy, diversity, separation or independence (if any) to the level credited in the safety analyses without prior NRC approval.

To ensure consistent application of this guidance, each of these characteristics is reviewed below.

Redundancy:

"Redundancy" means *two or more SSCs performing the same design function*.

The introduction of the exact same software into redundant channels and the potential creation of a software CCF has no impact on an SSCs' redundancy because the SSCs perform the same design function(s) before the introduction of software as they will after the introduction of software.

Diversity:

"Diversity" is not defined within the regulations as a stand-alone term. The term is defined within the context of GDC 22, as follows:

> "*Criterion 22 -- Protection system independence. The protection system shall be designed to assure that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function, or shall be demonstrated to be acceptable on some other defined basis.* ***Design techniques, such as functional diversity or diversity in component design and principles of operation****, shall be used to the extent practical to prevent loss of the protection function.*" [***emphasis*** added]

Commented [A56]: Enhancement: Supplement 1 to RIS 2002-22 establishes that reductions in redundancy, diversity and independence are general technical concerns for digital modifications and not specifically tied to any single evaluation criteria under 10 CFR 50.59. In order to properly align with Supplement 1, discussions regarding reductions in redundancy, diversity and independence should be stated at the beginning of the evaluation section for Appendix D.

Commented [A57]: Correction (b): These four terms are used in the Principle Design Criteria of many plants, in addition, they appear in standards incorporated by reference into the CFR as well as in RGs which some plants state (in the UFSAR) that they comply with. In short these terms are defined by the licensing basis of each plant, and they are not be defined in exactly the same way. Furthermore, the definitions of these terms below are inconsistent to their use in the GDCs and regulations incorporated by reference.

Commented [A58]: Correction (b): Suggest the revising the first sentence of this paragraph to: As discussed in NEI 96-07, Section 4.3.2, Example 6, a proposed activity that reduces redundancy, diversity, separation or independence of the design function.

For consistency with RIS 2002-22, Supplement 1, delete the second sentence, which is also inconsistent with the guidance in NEI 96-07.

Commented [A59]: Correction (b): GDC 22 is not a definition of diversity.

Suggested replacement language - "used as one example of a design technique"

Commented [A60]: Correction (b): The term "such as" should be understood in the same way as the term "for example" not like the term "that is" and therefore the term "such as" implicitly means that there are other modes of diversity, not just those listed.

Therefore, "diversity" is addressed in terms of *functional* or *component design and principles of operation*.

The introduction of the exact same software and the potential creation of a software CCF into single-failure proof channels, or merely redundant channels, has no impact on diversity because the channels were not initially diverse. Namely, each of the channels used the same principles of operation and they all contained identical components. Thus, the channels were identical before the introduction of software and will remain identical after the introduction of software.

Separation:

"Separation" refers to *physical arrangement* to provide missile protection, or to eliminate or minimize the detrimental impacts due to fires, floods, etc.

The introduction of the exact same software and the potential creation of a software CCF does not impact the physical arrangement of SSCs.

Independence:

"Independence" means *non-interaction* of SSCs.

Assuming that no interactions (e.g., communication between multiple applications of the software) exist, the introduction of the exact same software and the potential creation of a software CCF does not impact the independence of SSCs. However, the failure of such software due to a software CCF is possible and is addressed in Evaluation criterion #5 and/or #6.

Determination of Attributable (i.e., Causality)

NOTE: This guidance is not unique to digital and is the same as that provided in NEI 96-07, Section 4.3.2. This guidance is included here for completeness.

If none of the components/systems involved with the digital modification are identified as affecting a malfunction initiator previously identified in the UFSAR, then there is no attributable impact on the likelihood of occurrence of a malfunction.

Alternately, if any components/systems involved with the digital modification are identified as affecting a malfunction initiator previously identified in the UFSAR, then an impact on the likelihood of occurrence of a malfunction can be attributed to the digital modification. If an attributable impact is identified, then further assessment to determine the magnitude of the impact will be performed.

Example 4-13 illustrates a case of an *attributable* impact on the likelihood of

Commented [A61]: Correction (b): Delete this paragraph.
"Therefore" is inappropriate based on similar reasoning to that in the comment on the term "such as" above.

Commented [A62]: Correction (b): NRC staff is not clear on the intent of this paragraph. Staff recommends deleting this paragraph.
This statement is misleading and therefore will lead to regulatory uncertainty.

Protection systems should probably be dealt with differently than all other systems.

Commented [A63]: Correction (b): This definition is inconsistent with GDC 22, "*Protection system **independence***" which includes protecting redundant channels from being affected by the same cause.

Furthermore, the term "independence" is further elaborated in regulations and guidance.

This over simplification is not acceptable because it distorts the meaning.

Commented [A64]: Correction (b): Software CCF is a potential common cause for equipment failure, and is therefore potential source of reduced independence.

Commented [A65]: Correction (b): The term "malfunction initiator" is new and inappropriate because, in part:
(1) Generally only malfunctions are identified in the UFSAR, not the initiators of the malfunctions.
(2) it is not defined
(3) if question (ii) addresses "initiators" in the UFSAR, the question (vi) would be for all new ones, and the outcome threshold for question (vi) is lower than for questions (ii).

occurrence of a malfunction.

Example 4-13. ATTRIBUTABLE Impact on the Likelihood of Occurrence of a Malfunction

<u>Proposed Activity Description</u>

Two safety-related containment chillers exist. There are two analog control systems (one per chiller) 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 the same supplier and the software in each digital control system is exactly the same.

<u>Affected Malfunctions and Malfunction Initiators</u>

The affected malfunction is the failure of a safety-related containment chiller to provide its cooling design function. The UFSAR identifies three specific equipment-related initiators of a containment chiller malfunction: (1) failure of the Emergency Diesel Generator (EDG) to start (preventing the EDG from supplying electrical power to the containment chiller it powers), (2) an electrical failure associated with the chiller system (e.g., feeder breaker failure), and (3) a mechanical failure within the chiller itself (e.g., flow blockage). The UFSAR also states that the single failure criteria were satisfied because two chillers were provided and there were no common malfunction sources.

<u>Impact on Malfunction Likelihood</u>

Although the safety-related chiller control system is not one of the three malfunction initiators identified in the UFSAR, a new common malfunction source has been introduced due to the potential for a software common cause failure from the exact same software being used in both digital control systems. A common malfunction initiator was <u>previously considered</u>, but was concluded to be non-existent. However, this conclusion is no longer valid. Therefore, an impact on the likelihood of occurrence of the malfunction can be *attributed* to the digital modification. (NOTE: The magnitude of the impact would be assessed next.)

<u>Determination of Negligible/Discernable (i.e., Magnitude)</u>

NOTE: The guidance in this sub-section applies ONLY when an *attributable* impact on the likelihood of occurrence of a malfunction has been established.

For proposed activities in which there is an attributable impact on the likelihood of occurrence of a malfunction, the *negligible/discernable* portion of the criteria (i.e., magnitude) also needs to be assessed.

To determine the overall effect of the digital modification on the likelihood of a malfunction, an engineering evaluation is performed. An engineering evaluation that uses a qualitative assessment to judge the failure likelihood of the modified SSC should consider each factor identified below:

- Design attributes employed
- Quality of the design processes, and
- Operating experience of the software and hardware used (i.e., product maturity and in-service experience).

Negligible:

To achieve a *negligible* conclusion, the engineering evaluation of each factor (e.g., as documented in a qualitative assessment) would conclude that the affected SSC will exhibit a **sufficiently low** likelihood of failure, and by extension, that the change in the malfunction likelihood "...*is so small or the uncertainties in determining whether a change in likelihood has occurred are such that it cannot be reasonably concluded that the likelihood has actually changed (i.e., there is* ***<u>no clear trend toward increasing the likelihood)</u>***"[2] [***<u>emphasis</u>*** added].

Therefore, if the qualitative assessment outcome is **sufficiently low**, there is not more than a minimal increase in the likelihood of occurrence of a malfunction of an SSC important to safety previously evaluated in the UFSAR.

Discernable:

If the examination of each factor concludes that the change in the malfunction likelihood exhibits a clear trend towards increasing the likelihood, then a *discernable* increase in the malfunction likelihood would exist. In this case, the software CCF likelihood could be **sufficiently low** or **not sufficiently low**.

Commented [A66]: **Correction (b):** he failure likelihood cannot be both discernably increased and still be much lower than...

This same comment applies to Section 4.3.1.

Commented [A67]: **Correction (b):** Staff suggestion deletion of this sentence.

Conflicts with paragraph above. In short, this paragraph states that "a clear trend towards increasing" is not related to "sufficiently low" of software CCF.

Furthermore this paragraph seems to be inconsistent with the definition of sufficiently low in Section 3.15.

See similar comment above in Section 4.3.1. This same comment applies to Section 4.3.1 as the same logic is also used in that section for this concept.

The engineering evaluation (e.g., the qualitative assessment) is also used to determine if the discernible increase in the malfunction likelihood is "more than minimal" or "NOT more than minimal." To achieve a conclusion of "NOT more than minimal," the proposed activity must 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 I&C design modification and documented within the design modification package.

[2] Refer to NEI 96-07, Section 4.3.2, 4th paragraph.

Examples 4-14 and 4-15 illustrate the *negligible/discernable* portion (i.e., magnitude) of the criteria and assume the *attributable* portion of the criteria has been satisfied.

Example 4-14 illustrates a case with a *negligible* change to the malfunction likelihood.

Example 4-14. NEGLIGIBLE Impact in the Likelihood of Occurrence of a Malfunction

Proposed Activity Description

Two non-safety-related main feedwater pumps (MFWPs) exist, each with its own flow control valve. There are two analog control systems (one per MFWP 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 the same supplier and the software in each digital control system is exactly the same.

Magnitude Conclusion

A qualitative assessment performed as part of the design process, considering system design attributes, quality of the design processes employed, and operating experience of the proposed equipment, concluded that the failure likelihood of the modified SSC is **sufficiently low**.

All applicable requirements and other acceptance criteria to which the licensee is committed, as well as applicable design, material and construction standards, continue to be met.

Therefore, the change in the likelihood of occurrence of the loss of a MFWP or the closure of a MFWP flow control valve initiated by the failure of a feedwater control system is *negligible* due to the effect of the factors considered in the qualitative assessment.

Overall Conclusion

Although an attributable impact on the likelihood of occurrence of the loss of a MFWP or the closure of a MFWP flow control valve was determined to exist, there was no clear trend toward increasing the likelihood. With no clear trend toward increasing the likelihood, there is not more than a minimal increase in the likelihood of occurrence of the malfunctions due to the digital modification.

Example 4-15 illustrates a case with a *discernable* increase to the malfunction likelihood.

Example 4-15. DISCERNABLE Increase in the Likelihood of Occurrence of a Malfunction

Proposed Activity Description

Two safety-related main control room chillers exist. There are two analog control systems (one per chiller) 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 the same supplier and the software in each digital control system is exactly the same.

The logic components/system and controls for the starting and operation of the safety injection pumps are located within the main control room boundary. The environmental requirements associated with the logic components/system and controls are maintained within their allowable limits by the main control room cooling system, which includes the chillers involved with this digital modification.

Affected Malfunction and Malfunction Initiator

The review of the UFSAR accident analyses identified several events for which the safety injection pumps are assumed to start and operate (as reflected in the inputs and assumptions to the accident analyses).

In each of these events, the UFSAR states the following: "To satisfy single failure requirements, the loss of only one chiller control system and its worst-case effect on the event due to the loss of one chiller has been considered in the accident analyses."

Magnitude Conclusion

Based on the qualitative assessment performed as part of the technical assessment supporting this digital modification, the likelihood of a failure impacting both chiller control systems has been determined to be **not sufficiently low**.

The change in the likelihood of occurrence of the malfunction of both safety injection pumps is *discernable* due to the outcome of the qualitative assessment. Specifically, single failure criteria are no longer met.

Overall Conclusion

An attributable impact on the likelihood of occurrence of the malfunction of both safety injection pumps was determined to exist and there is a clear trend toward increasing the likelihood. The clear trend toward increasing the likelihood (i.e., the *discernable* increase) is due to the failure being **not**

sufficiently low which, in this case, causes single failure criteria to not be satisfied.

With a clear trend toward increasing the likelihood and failure to satisfy single failure criteria, there is more than a minimal increase in the likelihood of occurrence of the malfunction of both logic components/system and controls for the starting and operation of the safety injection pumps due to the digital modification.

HUMAN-SYSTEM INTERFACE ASSESSMENT

If no personnel-based initiators involving degraded operator performance (e.g., operator error) are identified among the malfunction initiators, then an increase in the likelihood of the malfunction cannot occur due to the Human-System Interface portion of the digital modification. Otherwise, the application of the *attributable* criterion (i.e., causality) and the *negligible/discernable* criterion (i.e., magnitude) are assessed utilizing the guidance described in NEI 96-07, Section 4.3.2.

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 96-07, Section 4.3.3 applies.

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 96-07, Section 4.3.4 applies.

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

INTRODUCTION

From NEI 96-07, Section 3.2:

> "*The term 'accidents' refers to the anticipated (or abnormal) operational transients and postulated design basis accidents...*"

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

From NEI 96-07, Section 4.3.5, the two considerations that need to be assessed when answering this Evaluation question are *as likely to happen as* and the *impact on the accident analyses* (i.e., a new analysis will be required or a revision to a current analysis is possible).

GUIDANCE

Determination of "As Likely To Happen As"

From NEI 96-07, Section 4.3.5:

> "*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.).*"

If the failure likelihood of the modified SSC is determined to be **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.

Alternately, if the failure likelihood of the modified SSC is determined to be **not sufficiently low**, then the activity does introduce failures that are *as likely to happen as* those in the UFSAR that can initiate an accident of a different type. In this case, further assessment to determine the impact on the accident analysis is to be performed.

Determination of Accident Analysis Impact

NOTE: This guidance is not unique to digital and is the same as that provided in NEI 96-07, Section 4.3.5, as clarified in RG 1.187.

For the case in which the creation of a possibility for an accident of a different type is as likely to happen as those in the UFSAR, the *accident analysis impact* also needs to be assessed to determine whether the accident is, in fact, a "different type."

There are two possible impacts on the accident analysis:

(1) a revision to an existing analysis is possible, or

(2) a new analysis will be required because the effect on the plant is different than any previously evaluated in the UFSAR

Commented [A68]: Correction (a): This paragraph appears to invoke the conclusion to rationale provided in Supplement 1 to RIS 2002-22 with regard to 10 CFR 50.59 (c)(2)(v). Without including some of the rationale prior to, this paragraph appears to jump to a conclusion.

Commented [A69]: Correction (b): Please explain why software CCF was changed to failure in this version of the document. Check redline strike version.

Commented [A70]: Enhancement: This phrase can be deleted because it is not needed and is ambiguous. That is as written, this sentence can be interpreted in more than one way. One such interpretation is, in short, not sufficiently low means there is an accident of a different type.

Commented [A71]: Enhancement: It would be more clear to simply replace this phrase with "whether the accident is of a different type."

Commented [A72]: Correction (b): Clarification of Section 4.3.5 of RG 1.187, as referenced here, has not been published. In order to avoid potential confusion and/or conflicts this guidance should be removed from this document.

Accidents of a different type are accidents that are as likely to happen as those in the UFSAR for which a new accident analysis would be needed, not just a revision of a current accident analysis.

Example 4-16 illustrates the NO CREATION of the possibility of an accident of a different type case.

Example 4-16. NO CREATION of the Possibility of an Accident of a Different Type

Proposed Activity

Two non-safety-related main feedwater pumps (MFWPs) exist, each with its own flow control valve. There are two analog control systems (one per MFWP 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 the same supplier and the software in each digital control system is exactly the same.

Malfunction / Accident Initiator

The malfunction/accident initiator identified in the UFSAR for the analog main feedwater control system is the loss of one main feedwater pump (out of two pumps) due to the loss of one feedwater control system.

Accident Frequency and Type

The pertinent accident is the Loss of Feedwater event. The characteristics of the Loss of Feedwater event are as follows:

Type of Accident - Decrease in Heat Removal by the Secondary System

Accident Category - Infrequent Incident

As Likely to Happen As Conclusion

Based on the qualitative assessment performed as part of the technical assessment supporting this digital modification, the failure likelihood of the modified SSC, causing the loss of both feedwater control systems (resulting in the loss of both MFWPs) has been determined to be **sufficiently low**.

Therefore, in this case, the creation of a possibility for an accident of a different type is NOT *as likely to happen as* those in the UFSAR and there is no need to determine the accident analysis impact.

Commented [A73]: Correction (a): The examples should follow the guidance. The guidance say the first thing you do is assess likelihood, and if sufficiently low, then you are done.

Therefore all of the material is not needed, and is misleading in that it implies that you do all of this first before you assess likelihood or even if any new accidents are “sufficiently low”.

Commented [A74]: Correction (a): - Consistency of language. Other example refer to this term as “engineering evaluation.”

Example 4-17 illustrates the CREATION of the possibility of an accident of a different type case.

Example 4-17. CREATION of the Possibility of an Accident of a Different Type

Proposed Activity

Two non-safety-related analog feedwater control systems and one non-safety-related main turbine steam-inlet valves analog control system exist.

The two feedwater control systems and the one main turbine steam-inlet valves control system will be combined into a single digital control system.

Malfunction / Accident Initiator

The identified feedwater control system malfunctions include (a) failures causing the loss of all feedwater to the steam generators [evaluated in the Loss of Feedwater event] and (b) failures causing an increase in main feedwater flow to the maximum output from both MFWPs [evaluated in the Excess Feedwater event].

The identified main turbine steam-inlet valve control system malfunctions include (a) all valves going fully closed causing no steam to be admitted into the turbine [evaluated in the Loss of Load event] and (b) all valves going fully open causing excess steam to be admitted into the turbine [evaluated in the Excess Steam Demand event].

Accident Frequency and Type

The characteristics of the pertinent accidents are as follows:

Loss of Feedwater:

Type of Accident - Decrease in Heat Removal by the Secondary System

Accident Category - Infrequent Incident

Excess Feedwater:

Type of Accident - Increase in Heat Removal by the Secondary System

Accident Category - Moderate Frequency Incident

Loss of Load:

Type of Accident - Decrease in Heat Removal by the Secondary System

Accident Category - Moderate Frequency Incident

Excess Steam Demand:

Type of Accident - Increase in Heat Removal by the Secondary System

Accident Category - Moderate Frequency Incident

As Likely to Happen As Conclusion

Commented [A75]: **Correction (a):** The examples should follow the guidance. The guidance say the first thing you go is assess likelihood, and if not sufficiently low, then you assess the impact. Much of the above information needed to assess the impact and therefore it should follow the likelihood evaluation.

Based on the qualitative assessment performed as part of the technical assessment supporting this digital modification, the failure likelihood of the modified SSC impacting both the feedwater control systems and the main turbine steam-inlet valves control system has been determined to be **not sufficiently low**.

Therefore, in this case, the following conditions are *as likely to happen as* those in the UFSAR, creating a possibility for several accidents:

(1) Loss of both feedwater pumps

(2) Increase in main feedwater flow to the maximum output from both MFWPs.

(3) All main turbine steam-inlet valves going fully closed

(4) All main turbine steam-inlet valves going fully open

(5) Combination of (1) and (3)

(6) Combination of (1) and (4)

(7) Combination of (2) and (3)

(8) Combination of (2) and (4)

Accident Analysis Impact Conclusion

Conditions (1) though (4) are already considered in the safety analyses, so a revision to an existing analysis is possible. Thus conditions (1) through (4) are NOT accidents of a different type.

The current set of accidents identified in the safety analyses does not consider a simultaneous Feedwater event (i.e., Loss of Feedwater or Excess Feedwater) with a Main Steam event (i.e., Excess Steam Demand or Loss of Load).

Condition (5) still causes a decrease in heat removal by the secondary system.

Condition (6) involves both a decrease and an increase in heat removal by the secondary system.

Condition (7) involves both a decrease and an increase in heat removal by the secondary system.

Condition (8) still causes an increase in heat removal by the secondary system.

Conditions (5) though (8) will require new accident analyses to be performed. As such, conditions (5) though (8) are accidents of a different type. Therefore, the proposed activity does create the possibility of accidents of a different type.

HUMAN-SYSTEM INTERFACE ASSESSMENT

If no personnel-based initiators involving degraded operator performance (e.g., operator error) are identified as accident initiators, then the creation of a possibility for an accident of a different type cannot occur due to the Human-System Interface portion of the digital modification. Otherwise, the creation of a possibility for an accident of a different type is assessed utilizing the guidance described in NEI 96-07, Section 4.3.5.

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

Commented [A76]: Correction (a): NRC staff is recommending the deletion of this section from Appendix D. However, should NEI wish to move forward with this section, the following comments will need to be resolved.

Commented [A77]: Correction (a): Contrary to 50.34(b), 50.59, and NEI 96-07. 50.34(b) states "The FSAR shall include information that describes the facility, presents the design bases and the limits on its operation, and presents the safety analyses **of the structures, systems and components** and of the facility as a whole." Appendix D incorrectly considers that "different result" related only to safety analysis for the "facility as a whole" but not to the safety analyses of the structures, systems and components. "NEI 96-07 definition for safety analyses states that also within the meaning of the definition are supporting UFSAR analyses that demonstrate SSC design functions will be accomplished as credited in the accident analyses." Malfunctions of structures, systems and components are generally postulated as potential single failures.

INTRODUCTION

NOTE: 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. Therefore, rather than simply providing supplemental guidance to that already included in NEI 96-07, Section 4.3.6, more detailed guidance will be provided in this section. However, none of the "more detailed" guidance provided in this section conflicts with that provided in NEI 96-07, Section 4.3.6, or should be construed as being *new*, or *modified* from that in NEI 96-07, Section 4.3.6.

Review

To ensure the unique aspects of digital modifications are addressed correctly and adequately, a review of selected discussions and excerpts from NEI 96-07, including *malfunctions*, *design functions*, and *safety analyses*, is presented first.

Commented [A78]: Correction (a): Partial quotations, taken out of context, maybe misinterpretations. It is far better to refer the reader to the original document, for careful study. That is, these partial quotations will lead to regulatory uncertainty.

These partial quotations are used to support conclusions for which the staff has concerns (e.g. NEI does not provide a rationale of why the quotes are being used.)

From NEI 96-07, Section 3.9:

> *"Malfunction of SSCs important to safety means the failure of SSCs to perform their intended* ***design functions*** *described in the UFSAR*

> *(whether or not classified as safety-related in accordance with 10 CFR 50, Appendix B)."* [***emphasis*** added]

From NEI 96-07, Section 3.3:

> *"Design functions are UFSAR-described **design bases functions** and other* SSC *functions described in the UFSAR **that support or impact design bases functions**..."* [***emphasis*** added]

Also,

> *"Design bases functions are functions performed by systems, structures and components (SSCs) that are (1) required by, or otherwise necessary to **comply with, regulations**, license conditions, orders or technical specifications, or (2) **credited in licensee safety analyses** to meet NRC requirements."* [***emphasis*** added]

Furthermore,

> *"Design functions...include functions that, **if not performed, would initiate a transient or accident that the plant is required to withstand**."* [***emphasis*** added]

Finally,

> *"As used above, "credited in the safety analyses" means that, if the SSC were not to perform its **design bases function** in the manner described, the assumed initial conditions, mitigative actions or other information in the analyses would no longer be within the range evaluated (i.e., the analysis results would be called into question). The phrase "support or impact design bases functions" refers both to those SSCs needed to support **design bases functions** (cooling, power, environmental control, etc.) and to SSCs whose operation or malfunction could adversely affect the performance of **design bases functions** (for instance, control systems and physical arrangements). Thus, both safety-related and nonsafety-related SSCs may perform design functions."* [***emphasis*** added]

This definition is oriented around the definition of design bases function, which itself is defined in NEI 97-04, Appendix B, "*Guidelines and Examples for Identifying 10 CFR 50.2 Design Bases*," endorsed by Regulatory Guide 1.186, and highlighted in bold above.

A more complete understanding of the meaning of a design basis function can be obtained by examination of NEI 97-04, Appendix B. From NEI 97-04, the three characteristics of design bases functions are summarized as follows:

1. Design bases functions are credited in the safety analyses.

2. The functions of any individual SSC are functionally below that of a design basis function.
3. Design bases functions are derived primarily from the General Design Criteria.

Repeating a portion from above to highlight the importance of identifying the design basis function and its connection to a safety analysis result, we have the following:

Commented [A79]: **Correction (a):** 10 CFR 50.59 is about design functions, not a subset of design functions. By focusing on a "design basis function and its connections to a safety analysis result" an implementer may understand this guidance as directing him to ignore the other design functions and other results.

The NRC made a presentation in a public meeting on November 30, 2017 (ML17335A574), which expressed concern with this approach.

This section should be revised to provide fuller context of quotes or deleted per general comment above re: this section.

> *"As used above, "credited in the safety analyses" means that, if the SSC were not to perform its design bases function in the manner described, the assumed initial conditions, mitigative actions or other information in the analyses would no longer be within the range evaluated* ***(i.e., the analysis results would be called into question)****."* [***emphasis*** added]

Then, from NEI 96-07, Section 3.12:

> *"****Safety analyses*** *are analyses performed pursuant to NRC requirements to demonstrate the integrity of the reactor coolant pressure boundary, the capability to shut down the reactor and maintain it in a safe shutdown condition, or the capability to prevent or mitigate the consequences of accidents that could result in potential offsite exposures comparable to the guidelines in 10 CFR 50.34(a)(1) or 10 CFR 100.11...and include, but are not limited to, the* ***accident analyses*** *typically presented in Chapter 15 of the UFSAR."* [***emphasis*** added]

And from the first sentence of the associated discussion:

> *"Safety analyses are those analyses or evaluations that* ***demonstrate that acceptance criteria*** *for the facility's capability to withstand or respond to postulated events* ***are met****."* [***emphasis*** added]

Failure Modes and Effects Analysis (FMEA)

NEI 96-07, Section 4.3.6 recognizes that the effect of a proposed modification must be assessed. This assessment may require the use of a failure modes and effects analysis (FMEA), including the possible creation of a new FMEA.

From NEI 96-07, Section 4.3.6:

> *"In evaluating a proposed activity against this criterion, the types and results of failure modes of SSCs that have previously been evaluated in the UFSAR and that are affected by the proposed activity should be identified. This evaluation should be performed consistent with any failure modes and effects analysis (FMEA) described in the UFSAR,*

> *recognizing that **<u>certain proposed activities may require a new FMEA to be performed.</u>**"* [***<u>emphasis</u>*** added]

<u>Overall Perspective</u>

NEI 96-07, Section 4.3.6 provides the overall perspective on this Evaluation criterion with its first sentence, which states:

> *"Malfunctions of SSCs are generally postulated as potential single failures to evaluate plant performance with the focus being on the result of the malfunction rather than the cause or type of malfunction."*

Expanding upon this foundation, the following conclusion is reached, which is based upon discussion from 63 FR 56106:

> *Unless the equipment would fail in a way **<u>not already evaluated in the safety analysis</u>**, there can be no malfunction of an SSC important to safety with a different result.* [***<u>emphasis</u>*** added]

From NEI 96-07, Section 4.3.6, there are two considerations that need to be assessed when answering this criterion: *as likely to happen as* and *impact on the safety analysis result*.

<u>GUIDANCE</u>

<u>Determination of "As Likely to Happen As"</u>

From NEI 96-07, Section 4.3.6:

> *"The possible malfunctions with a different result are limited to those that are **<u>as likely to happen as those described in the UFSAR</u>**…a proposed change or activity that increases the likelihood of a malfunction previously thought to be incredible to the point where it becomes as likely as the malfunctions assumed in the UFSAR could create a possible malfunction with a different result."* [***<u>emphasis</u>*** added]

If the failure likelihood of the modified SSC is determined to be **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 other previously evaluated in the UFSAR.

Alternately, if the failure likelihood of the modified SSC is determined to be **not sufficiently low**, then the activity does introduce failures that are *as likely to happen as* those in the UFSAR. In this case, further assessment to determine the impact of the malfunction on the safety analysis result is to be performed.

Example 4-18 illustrates the NO CREATION of the possibility for a malfunction with a different result due to applying the *as likely to happen as* consideration.

Example 4-18. NO CREATION of the Possibility for a Malfunction with a Different Result

Proposed Activity

A large number of analog transmitters 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.

Conclusion

Based on the qualitative assessment, the failure likelihood of the modified SSC has been determined to be **sufficiently low**.

Therefore, a malfunction with a different result is NOT *as likely to happen as* those described in the UFSAR and there is no need to determine the impact of the malfunction on the safety analysis result. Thus, the proposed activity does NOT create the possibility for a malfunction of an SSC important to safety with a different result.

Determination of Safety Analysis Result Impact

The generic process to determine the impact of a malfunction of an SSC important to safety on the safety analyses, i.e., a comparison of the safety analyses results to identify any different results, consists of multiple steps, as summarized next.

Step 1: Identify the functions directly or indirectly related to the proposed modification.

Considering the scope of the proposed digital modification, identify the functions that are directly or indirectly related to the proposed activity.

Step 2: Identify which of the functions from Step 1 are Design Functions and/or Design Bases Functions.

Utilizing NEI 96-07, Section 3.3, classify the functions from Step 1. If no *design functions* are identified, then the proposed activity does NOT create the possibility for a malfunction of an SSC important to safety with a different result.

Utilizing NEI 96-07, Section 3.3, along with Appendix B to NEI 97-04, as needed, identify which *design functions* are *design bases functions*, which *design functions* "support or impact" *design bases functions,* and which *design functions* are not involved with *design bases functions,*

Commented [A80]: Correction (a): This is an open issue documented in the meeting summary from the 11/30/2017 public meeting (ML17331A485), which states:

The NRC staff pointed out that Title 10 to the Code of Federal Regulations (10 CFR), Section 50.59, (10 CFR 50.59) "Changes, test and experiments," used the term "final safety analysis report (as updated)" while NEI 96-07, Appendix D, Section 4.3.6 used the terms "safety analysis" and "accident analysis." The NRC staff said that it could be understood that "accident analysis" is a subset of "safety analysis" which is a subset of "final safety analysis report (as updated)." Using more restrictive terms, it could be understood that the evaluation guidance only addressed a subset of "any [malfunction] previously evaluated in the final safety analysis report (as updated)."

but are functions that if not performed would initiate a transient or accident that the plant is required to withstand. If no *design basis functions* are involved, proceed to Step 5.

The process for determining if a *design function* is a *design basis function* is aided by identifying the associated General Design Criteria (GDC) to which a *design bases function* applies. Each design function can then be related to the requirements discussed within the GDC to determine if that *design function* is directly involved with the *design basis function* itself or if the *design function* "supports or impacts" the related *design basis function*. If the *design function* is found to directly involve the GDC requirement, then that *design function* is a *design basis function*. If the *design function* "supports or impacts" the GDC requirement, then it is not a *design basis function*, but is still "credited in the safety analysis."

Step 3: Determine if a new FMEA needs to be generated.

If the impact on the *design basis function* involved is readily apparent, no new FMEA needs to be generated, skip this step and go to Step 4. For example, there is no reason to contemplate the generation of a new FMEA if the impact of the failure on the *design bases functions* is recognized as being immediate. Otherwise, generate the new FMEA to describe the connection of the proposed activity, or failures due to the proposed activity, to an impact on the *design bases functions*.

As part of the process for generating the new FMEA, presume compliance with pre-existing/interdependent, modification-related procedures and utilization of existing equipment to determine if adequate options exist to mitigate potential detrimental impacts on *design functions*.

"Interdependence" is discussed in NEI 96-07, Sections 4.2 and 4.3. An example of an interdependent procedure change would be the modifications to an existing procedure to reflect operation of the new digital equipment and controls, including any new features such as a control system restart option.

Step 4: Determine if each design basis function continues to be performed/satisfied.

If all *design basis functions* continue to be performed/satisfied, and there are no other *design functions* involved, then the proposed activity does NOT create the possibility for a malfunction of an SSC important to safety with a different result.

Commented [A81]: Correction (a): The meeting summary from the 11/30/2017 public meeting (ML17331A485), states:
"The NRC staff noted that Step 2 did point to the appropriate guidance for identifying design bases functions, more specific guidance used the 10 CFR General Design Criteria (GDC) for identification purposes. The NRC staff said that a subset of design bases function can be tied to the GDC. NEI stated that the vast majority of design basis functions are derived from the GDCs."

The NRC made a presentation in the public meeting on November 30, 2017 (ML17335A574), which expressed concern with "Using GDCs to Identify Design Basis Functions Vs. UFSAR to Identify Design Functions"

Based on these interactions, the NRC and NEI are still at an impasse over this issue.

Commented [A82]: Correction (a):
NEI 96-07, Revision 1, Section 4.3.2, Example 4, provides guidance on new operator actions as follows with regards to interdependence:

The change involves a new or modified operator action that supports a design function credited in safety analyses [would not require prior NRC approval] provided:

- The action (including required completion time) is reflected in plant procedures and operator training programs

- The licensee has demonstrated that the action can be completed in the time required considering the aggregate affects, such as workload or environmental conditions, expected to exist when the action is required.
  - To illustrate this point - *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.*

- The evaluation of the change considers the ability to recover from credible errors in performance of manual actions and the expected time required to make such a recovery.

...

Commented [A83]: Correction (a):
Please clarify the concept to "adequate options". NEI 01-01 specifically references "adequate *backups*" with regard the determination of potential new outcomes and effects on design functions being preserved or not. It's not clear how a system restart or reboot constitutes an "adequate backup" to the potentially failed SSC.

As oppose to using the term "adequate options should be replaced with specific guidance that described acceptable options, which are already provided in NEI 96-07, Revision 1, Section 4.3.2, Example 4.

Specific compensatory measure, such as opening doors, turning on fans, or installing temporary fans, is not acceptable because those actions are not interdependent with the modifications, in that the actions were added with the purpose of avoiding a license amendment.

...

For any *design basis function* that does not continue to be performed/satisfied, or other *design functions* that are involved, continue to Step 5.

Step 5: Identify all safety analyses involved.

Identify all safety analyses that rely directly or indirectly on the *design basis function's* performance/satisfaction. Also, identify all safety analyses related to any other *design function* that could impact either the accident's initiation or the event's initial conditions, i.e., *design functions* that, if not performed, would initiate a transient or accident that the plant is required to withstand.

If there are no safety analyses involved, then there has been no change in the result of a safety analysis and the proposed activity does NOT create the possibility for a malfunction of an SSC important to safety with a different result.

Commented [A84]: Correction (a): Contrary to NEI 96-07 and 10 CFR 50.59.

NEI 96-07, section 4.3.6.2, states The safety analysis assume certain design functions of SSCs in demonstrating the adequacy of the design. Thus, certain design functions, while not specifically identified in the safety analysis, are credited in a direct sense."

Commented [A85]: Correction (a):
Questions (vi) and (vi) are meant to address "new' or different accidents and malfunctions; there will never be any "pre-existing safety analysis" for new types of events created by a change. Based upon the reasoning stated here, it could be potentially be understood that malfunctions such as CCF would not be considered a different result if not previously analyzed. This would be contrary to Questions (vi) under 50.59.

Not all design functions are credited in the safety analysis. Some design functions are required for other reasons (e.g., to meet regulations).

Some design functions exist to prevent the possibility of a DBA or AOO (e.g., control rod withdrawal prohibit or permissive); therefore no safety analysis exists for said DBA or AOO.

Example 4-21 points to one of the concerns with the reasoning embodied in this step. One of the ideas is that a change should not more than minimally impact the "consequences" which in 50.59 means dose. "Consequences" is a subset of "results". Radiation monitors are used, in part, to limit dose, so a misbehavior in that system could adversely impact dose.

Step 6: For each safety analysis involved, compare the projected/postulated results with the previously evaluated results.

NEI 96-07, Section 4.3.6 provides the following guidance regarding the identification of failure modes and effects:

> *"Once the malfunctions previously evaluated in the UFSAR and the results of these malfunctions have been determined, then the types and results of failure modes that the proposed activity could create are identified."*

If any of the identified safety analyses have become invalid due to their basic assumptions no longer being valid (e.g., single failure assumption is not maintained), or if the numerical result(s) of any safety analysis would no longer satisfy the acceptance criteria, then the proposed activity DOES create the possibility for a malfunction of an SSC important to safety with a different result.

As part of the response and determining if the safety analyses acceptance criteria continue to be satisfied, include the impact on the severity of the initiating conditions and the impact on the initial conditions assumed in the safety analysis. Specifically, consider any *design functions* that, if not performed, would initiate a transient or accident that the plant is required to withstand.

Examples 4-19 through 4-24 illustrate cases in which the failure likelihood of the modified SSC is determined to be **not sufficiently low** and, by extension, the likelihood of a software CCF is also determined to be **not sufficiently low**, i.e., a malfunction is *as likely to happen as* those described in the UFSAR. In these cases, the multi-step process applying the "safety analysis result impact" consideration is performed to determine the impact of the malfunction on the safety analysis result.

Examples 4-19 through 4-23 illustrate some cases of NO CREATION of a malfunction with a different result.

Example 4-19. NO CREATION of a Malfunction with a Different Result

Proposed Activity

A feedwater control system is being upgraded from an analog system to a digital system. New components are being added that could fail in ways other than the components in the original design. Now, as a result of this change, all four feedwater flow control valves could simultaneously fail closed following a software CCF.

Safety Analysis Result Impact Consideration

Step 1:

The identified function is to establish and maintain steam generator water level within predetermined physical limits during normal operating conditions.

Step 2:

The function is classified as a design function due to its ability to "…initiate a transient or accident that the plant is required to withstand." However, the design function is not a design basis function. With no design basis functions involved, proceed to Step 5.

Step 3:

Not applicable

Step 4:

Not applicable

Step 5:

The pertinent safety analysis is the accident analysis for Loss of Feedwater. The feedwater control system has a direct impact on the accident analysis assumptions and modeling.

Step 6:

The severity of the initiating failure for the Loss of Feedwater is unchanged. The event already assumes a total loss of feedwater flow. The newly created failure modes are determined to have no effect on this assumption. The manner in which feedwater flow is lost has no impact on the initial conditions of the event.

Conclusion

Although the software CCF likelihood was determined to be **not sufficiently low** (i.e., a malfunction is *as likely to happen as* those described in the UFSAR), the initiation severity of the Loss of Feedwater event, the newly created failure modes and the manner in which feedwater flow was lost do not change the result of the safety analysis. Thus, the proposed activity does NOT create the possibility for a malfunction of an SSC important to safety with a different result.

Example 4-20. NO CREATION of a Malfunction with a Different Result

Proposed Activity

A feedwater control system is being upgraded from an analog system to a digital system. Previously, only one of four feedwater flow control valves was assumed to fail open as part of the initiation of the Excess Feedwater event. Now, as a result of this change, all four feedwater flow control valves could simultaneously fail open following a software CCF.

Safety Analysis Result Impact Consideration

Step 1:

The identified function is to establish and maintain steam generator water level within predetermined physical limits during normal operating conditions.

Step 2:

The function is classified as a design function due to its ability to "…initiate a transient or accident that the plant is required to withstand." However, the design function is not a design basis function. With no design basis functions involved, proceed to Step 5.

Step 3:

Not applicable

Step 4:

Not applicable

Step 5:

The pertinent safety analysis is the accident analysis for Excess Feedwater. The feedwater control system has a direct impact on the accident analysis assumptions and modeling.

Step 6:

The severity of the initiating failure has increased due to four valves supplying flow as compared to one valve prior to the change.

The minimum allowed departure from nucleate boiling ratio (DNBR) to satisfy the accident analysis acceptance limit is 1.30. The current minimum DNBR result is 1.42. After using an increased value for the new feedwater flow (to represent the increase in feedwater flow caused by the opening of the four feedwater flow control valves) in a revision to the Excess Feedwater accident analysis, the new minimum DNBR result is 1.33.

Conclusion

Although the software CCF likelihood was determined to be **not sufficiently low** (i.e., a malfunction is *as likely to happen as* those described in the UFSAR) and the severity of the initiating failure has increased, the new minimum DNBR result continues to satisfy the accident analysis acceptance limit, which does not change the result of the safety analysis. Therefore, the proposed activity does NOT create the possibility for a malfunction of an SSC important to safety with a different result.

Commented [A86]: Correction (a): Contrary to 10 CFR 50.59 regulation and NEI 96-07 which states that the results must be bounded by the previous analysis, not accident analysis acceptance criteria.

Example 4-21. NO CREATION of a Malfunction with a Different Result

Proposed Activity

A complete system upgrade to the area radiation monitors that monitor a variety of containment compartments that could be subject to radioactive releases during a LOCA is proposed. The outdated analog-based radiation monitors are being replaced by digitally-based monitors. The hardware platform for each area radiation monitor is from the same supplier and the software in each area radiation monitor is exactly the same.

Safety Analysis Result Impact Consideration

Step 1:

The functions include the monitoring of the various compartments, rooms and areas that may be subject to an increase in radiation during the recirculation phase of a LOCA.

Step 2:

In this case, whether the function is a design bases function is not readily determined, so the associated GDC will be identified and examined.

> *Criterion 64 -- Monitoring radioactivity releases. Means shall be provided for* ***monitoring*** *the reactor containment atmosphere,* ***spaces containing components for recirculation of loss-of-coolant accident fluids****, effluent discharge paths, and the plant environs* ***for radioactivity*** *that may be released from normal operations, including anticipated operational occurrences, and from postulated accidents.* [***emphasis*** added]

The area radiation monitors perform a function that is necessary to comply with a requirement specified in GDC 64. Therefore, the radiation monitor's function is directly involved with a design basis function.

Step 3:

No new FMEA needs to be generated. The effect of a postulated software CCF on the design basis function involved is readily apparent.

Step 4:

If a software CCF occurs, the area radiation monitors will not perform their design function that supports or impacts a design basis function. Thus, the design basis function will not be performed/satisfied.

Step 5:

There are no safety analyses that directly or indirectly credit this design basis function. That is, there are no considerations of malfunctions of single or multiple radiation monitors in any safety analysis.

Step 6:

Not applicable

<u>Conclusion</u>

The cited GDC does not contain any reference to single failure protection, so there is no distinction between a failure of a single radiation monitor or multiple radiation monitors.

Although the software CCF likelihood was determined to be **not sufficiently low** (i.e., a malfunction is *as likely to happen as* those described in the UFSAR), there are no safety analyses that directly or indirectly credit the design basis function. Thus, there cannot be a "different result" when comparing to a pre-existing safety analysis since none exists.

Therefore, the proposed activity does NOT create the possibility of a malfunction of an SSC important to safety with a different result.

NOTE: The acceptability of these new area radiation monitors will be dictated by their reliability, which is assessed as part of Criterion #2, not Criterion #6.

Commented [A87]: Correction (a): This example points one of the concerns with the reasoning embodied in the multi-step process. One of the ideas is that a change should not more than minimally impact the "consequences" which in 50.59 means dose. "Consequences" is a subset of "results". The radiation monitors are used, in part, to limit dose, so a misbehavior in that system could adversely impact dose.

Questions (vi) and (vi) are meant to address "new' or different accidents and malfunctions; there will never be any "pre-existing safety analysis" for new types of events created by a change.

Example 4-22. NO CREATION of a Malfunction with a Different Result

Proposed Activity

Two chillers that cool the Main Control Room Ventilation System (MCRVS) are being upgraded. As part of the upgrade, each analog control system will be replaced with a digital control system. Each digital control system maintains all of the operational features (e.g., auto/manual start/stop, setpoints and alarms) as the analog control systems. The hardware platform for each chiller control system is from the same supplier and the software in each chiller control system is exactly the same.

Safety Analysis Result Impact Consideration

Step 1:

The MCRVS also cools the Relay Room that is adjacent to the main control room. The Relay Room contains multiple instrument racks that control both Reactor Protection and Safeguards actuation signals. The air flow path from the Main Control Room to the Relay Room is described in the UFSAR, along with a function to maintain the Relay Room's temperature less than or equal to 120 °F.

Step 2:

In this case, whether the function is a design bases function is not readily determined, so the associated GDC will be identified and examined.

> *Criterion 20 -- Protection system functions. The protection system shall be designed (1)* ***to initiate automatically the operation of***

> ***appropriate systems including the reactivity control systems****, to assure that specified acceptable fuel design limits are not exceeded as a result of anticipated operational occurrences and (2)* ***to sense accident conditions and to initiate the operation of systems and components important to safety****.* [***emphasis*** added]

The chillers and the chiller control systems perform a function that supports or impacts the design basis function specified in GDC 20. Therefore, the chillers and the chillers control systems' functions are design functions "credited in the safety analysis."

Step 3:

The impact of a software CCF on the design bases functions is not readily apparent, so a new FMEA was generated.

Step 4:

The new FMEA concluded that compliance with pre-existing procedures will result in the restoration of at least one chiller well before the Relay Room cooling becomes inadequate. Specifically, compliance with existing procedures will direct the recognition of the problem and the restoration of the chiller's function prior to the impairment of the associated design basis functions. In addition, an interdependent procedure change involved the use of the control system "restart" feature to reinitialize the control system, which would clear any software faults, allowing the chiller functions to be restored well before the Relay Room cooling becomes inadequate.

Commented [A88]: **Correction (a):** See comment above on Interdependence. It's not clear that, based upon the guidance on Interdependence above and the content presented in this example, that the example adequately captures the necessary aspects of interdependence procedural changes. Also reflects staff's concerns with partial quotations from NEI 96-07 out of context that potentially leads to misinterpretations and ultimately, regulatory uncertainty.

Step 5:

Although none of the safety analyses specifically identify assumptions or inputs related to the MCRVS, the Relay Room or the components therein, several accident analyses assume correct and timely actuation of the Reactor Protection and Safeguards features. As determined in Step 2 above, the chillers' operation is considered to be "credited in the safety analysis" since they "support or impact" the design bases functions associated with GDC 20. As demonstrated as part of Step 4, all design basis functions are preserved.

Step 6:

As determined in Step 4, all design basis functions are preserved. Therefore, all of the safety analyses identified in Step 5 remain valid and there is no change in any safety analysis result.

<u>Conclusion</u>

Although the software CCF likelihood was determined to be **not sufficiently low** (i.e., a malfunction is *as likely to happen as* those described in the UFSAR), the design bases functions will continue to be performed/satisfied and the safety analyses (and all of the results from these analyses) are unaffected. Therefore, the proposed activity does NOT create the possibility of a malfunction of an SSC important to safety with a different result.

Example 4-23. NO CREATION of a Malfunction with a Different Result

Proposed Activity

Currently, the feedwater control system and the pressurizer pressure control system are separate analog control systems.

The feedwater control system is being upgraded from an analog to a digital system. Previously, only one of four feedwater flow control valves was assumed to fail open as part of the initiation of the Excess Feedwater event. Now, as a result of this change, all four feedwater flow control valves could simultaneously fail open following a software CCF.

The pressurizer pressure control system is being upgraded from an analog to a digital system.

As part of this modification, the two previously separate control systems will be combined within the same digital controller in a distributed control system (DCS) with the same software controlling all feedwater and pressurizer functions.

Safety Analysis Result Impact Consideration

Step 1:

Feedwater - The identified function is to establish and maintain steam generator water level within predetermined physical limits during normal operating conditions.

Pressurizer - The identified function is control of the pressurizer sprays and heaters.

Step 2:

Feedwater - The function is classified as a design function due to its ability to "…initiate a transient or accident that the plant is required to withstand." However, the design function is not a design bases function.

Pressurizer - In this case, whether the function is a design bases function is not readily determined, so the associated GDC will be identified and examined.

> *Criterion 10 -- Reactor design. The reactor core and associated coolant, control, and protection systems shall be designed with appropriate margin to assure that specified acceptable fuel design limits are* ***not exceeded during any condition of normal operation, including the effects of anticipated operational occurrences.*** [***emphasis*** added]

The pressurizer control system performs a function that "supports or impacts" a design basis function specified in GDC 10. Therefore, the pressurizer control system's function is a design function and is "credited in the safety analysis."

Step 3:

The effect on the feedwater and pressurizer control systems is clear and understood, having a direct impact on the accident analysis assumptions and modeling. There is no reason to contemplate the generation of a new FMEA since the impact of the software CCF on the accident analysis is readily apparent (i.e., clear and understood).

Step 4:

If a software CCF occurs, the pressurizer pressure control function, which supports or impacts the GDC 10 design basis function, will not continue to be performed/satisfied.

Commented [A89]: **Correction (a):**

Please clarify in this step why only the impact on pressurizer pressure controls is considered affected by a software CCF when step 1 clearly states that pressurizer and feedwater controls are integrated into the same DCS. What is the basis for only pressurizer controls being affected?

See GDC comment on page D-47 of this document.

Step 5:

The pertinent safety analysis is the accident analysis for Excess Feedwater. Typically, in Chapter 15 accident analyses control system action is considered only if that action results in more severe accident results. The feedwater and pressurizer control systems have a direct impact on the accident analysis assumptions and modeling.

Step 6:

In the Excess Feedwater accident analysis, **the initial conditions already assume abnormally low pressure and/or DNBR.** Since the pressurizer pressure control system would mitigate the results of the accident, no credit is taken for operation of the pressurizer pressure control system. Therefore, a malfunction of the control system would have no effect on this event and no effect on the safety analysis result.

The severity of the initiating failure is not affected due to the combination of the two control systems. The minimum allowed DNBR to satisfy the accident analysis acceptance limit is 1.30. The current minimum DNBR result is 1.42. After using an increased value for the new feedwater flow (to represent the increase in feedwater flow caused by the opening of the four feedwater flow control valves) and adjusting the appropriate inputs to reflect the new detrimental pressurizer heater and spray conditions in a revision to the Excess Feedwater accident analysis, the new minimum DNBR result is 1.33.

Conclusion

With the software CCF likelihood determined to be **not sufficiently low** (i.e., a malfunction is *as likely to happen as* those described in the UFSAR), the severity of the initiating failure has increased. The impairment of the pressurizer pressure control function is already incorporated in the safety analysis' modeling. The new minimum DNBR result continues to satisfy the accident analysis acceptance limit, which does not change the result of the safety analysis. Therefore, the proposed activity does NOT create the possibility of a malfunction of an SSC important to safety with a different result.

Commented [A90]: Correction (a): This example and conclusion appears to presume that, a DCS with combined functionality of different SSC design functions will still fail in a preexisting or known way such as the pressurizer sprays, heaters, etc. would still fail in a previously anticipated way even though a different technology is now controlling its functionality and is no longer a separate function. It's not clear that this example takes into account spurious actuation of various components of the system or whether the example consider the Chapter 15 analysis as the still most limiting failure for the DCS.

Commented [A91]: Correction (a): See comments previously stated in example 4-20.

Example 4-24 illustrates a case in which there is the CREATION of a malfunction with a different result.

Example 4-24. CREATION of a Malfunction with a Different Result

Proposed Activity

An upgrade to the analog-based reactor protection system with a digital-based reactor protection system is proposed. This proposed modification involves replacement of all the solid state cards that control the detection of anticipated operational occurrences and the actuation of the required reactor trip signals. Redundant channels contain these cards in satisfaction of single failure criteria.

Safety Analysis Result Impact Consideration

Step 1:

The number of involved functions is large, all of which involve the detection of the occurrence of anticipated operational occurrences, the processing of those signals, and the generation of the appropriate reactor trip signals.

Step 2:

In this case, whether the functions are design bases function is not readily determined, so the associated GDCs will be identified and examined.

> *Criterion 20 -- Protection system functions. The protection system shall be designed (1)* ***to initiate automatically the operation of appropriate systems including the reactivity control systems****, to assure that specified acceptable fuel design limits are not exceeded as a result of anticipated operational occurrences and (2)* ***to sense accident conditions and to initiate the operation of systems and components important to safety****.* [***emphasis*** added]
>
> *Criterion 21 -- Protection system reliability and testability. The protection system shall be designed for high functional reliability and inservice testability commensurate with the safety functions to be performed. Redundancy and independence designed into the protection system shall be sufficient to assure that (1)* ***no single failure results in loss of the protection function*** *and (2) removal from service of any component or channel does not result in loss of the required minimum redundancy unless the acceptable reliability of operation of the protection system can be otherwise demonstrated. The protection system shall be designed to permit periodic testing of its functioning when the reactor is in operation, including a capability to test channels independently to determine failures and losses of redundancy that may have occurred.* [***emphasis*** added]
>
> *Criterion 22 -- Protection system independence. The protection system shall be designed* ***to assure that the effects of*** *natural phenomena, and of* ***normal operating****, maintenance, testing, and postulated accident* ***conditions on redundant channels do not result in loss of the protection function****, or shall be demonstrated to be acceptable on some other defined basis. Design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protection function.* [***emphasis*** added]

The components perform functions that support or impact design bases functions specified in GDCs 20, 21, and 22. Thus, these functions are design functions and are “credited in the safety analysis.”

Step 3:

The effect on the detection, processing and generation of signals is clear and understood, having a direct impact on the safety analysis assumptions. There is no reason to contemplate the generation of a new FMEA since the impact of the software CCF on the design bases functions is readily apparent (i.e., clear and understood).

Step 4:

Performance/satisfaction of the design bases functions related to the GDC 21 and 22 requirements regarding single failure criteria and redundant channels will not continue to be performed/satisfied.

Step 5:

Numerous safety analyses contain implicit assumptions regarding the performance and/or expectation of the minimum number of system/components and/or trains/channels that are expected to perform their function, which satisfy the applicable redundancy requirements and/or single failure criteria.

Step 6:

In all cases for each safety analysis, the inability to satisfy the performance and/or expectation of the minimum number of systems/components and/or trains/channels violates an assumption upon which the safety analysis results are based.

In these instances, a simple review of the safety analyses and their structure will quickly identify that the results will exceed the associated acceptance criteria.

Conclusion

With the software CCF likelihood determined to be **not sufficiently low** (i.e., a malfunction is *as likely to happen as* those described in the UFSAR), the assumptions regarding satisfaction of single failure criteria are invalidated. Therefore, the proposed activity DOES create the possibility of a malfunction of an SSC important to safety with a different result.

HUMAN-SYSTEM INTERFACE ASSESSMENT

If no personnel-based initiators involving degraded operator performance (e.g., operator error) are identified as malfunction initiators, then the creation of a possibility for a malfunction of an SCC important to safety with a different result cannot occur due to the Human-System Interface portion of the digital modification. Otherwise, the creation of a possibility for a malfunction of an SSC important to safety with a different result is assessed utilizing the guidance described in NEI 96-07, Section 4.3.6.

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. The guidance in NEI 96-07, Section 4.3.7 applies.

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. The guidance in NEI 96-07, Section 4.3.8 applies.

5.0 EXAMPLES

[LATER]