NEI 96-07, Appendix D
Draft Revision 0d

Commented [A1]: Comment Legend:
COMMENT (5) - Observation by NRC with no suggested change
CONSISTENT with PRIOR COMMENT (15) - Previously, the NRC had made a conceptual comment, but may not have identified this specific instance for change.
COMMENT on IMPLEMENTATION (12) - In the last direct edit meeting, it was agreed that NEI would make certain changes after the meeting. These are NRC corrections to those changes.
EDITORIAL (9) - Editorial changes (by NRC) with no change in meaning intended.
NEW (5) - Comment not discussed at last meeting.
NEW SUGGESTION (9) - NRC suggestion not discussed at last meeting.
SUGGESTED CHANGE (18) - NRC suggestion for improvement.
UNDELETED & EDITED (3) - Text was deleted by NEI after the last direct edit meeting. NRC suggests un-deletion; therefore the NRC undeleted it. Subsequent NRC editorial changes are shown with track changes.

Nuclear Energy Institute

SUPPLEMENTAL GUIDANCE FOR APPLICATION OF 10 CFR 50.59 TO DIGITAL MODIFICATIONS

Commented [A2]: Thematic Concerns:
Software CCF: Maintain consistency in terminology through document.

Design Function Condition: Concept is not needed for screening or evaluation of impacts to Diversity, Independence, …

UFSAR Described: Additional deletion of terms per prior comment.

Qualitative Assessment: Incomplete implementation of prior agreement to remove partial qualitative assessment guidance

HFE: Deletion of additional examples & minor edits

October 2017

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 NEI 01-01/ EPRI TR-102348, Guideline on Licensing of Digital Upgrades.~~

Commented [A3]: NEW: Previously the plan was to release "licensing" and "technical" guidance to replace NEI 01-01, but recently, a decision was made to release for use only the "licensing" guidance, which makes this statement no longer correct.

NEI 01-01 addresses both technical and licensing aspects. This document only addresses licensing aspects.

Furthermore, if endorsed by a letter, both documents will be usable.

TABLE OF CONTENTS

1 INTRODUCTION

There are specific considerations that should be addressed as part of the 50.59 process when performing 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 ~~(SCCF))~~.

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

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.

Commented [A4]: EDITORIAL: NEI made this editorial change after the September Direct Edits meeting. NRC staff suggests this is not needed and is less clear. Furthermore, some changes to the document are preferable to ensure consistent use of terminology.

Previously, this document was inconsistent in how it referred to software CCF. NRC staff edited the use of "software CCF" to be consistent throughout the document.

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.

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 modifications 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 Devices 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.

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[1]. 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.

Commented [A5]: CONSISTENT with PRIOR COMMENT: Deleting "UFSAR-described" here is appropriate because it is consistent with Screening guidance. Use of "UFSAR-described" elsewhere is appropriate in that it accurately conveys something must be explicitly described (i.e. not indirect effects).

Commented [A6]: NEW SUGGESTION: NRC staff added a footnote for clarification.

As the footnote explains "design function" is defined in NEI 96-07. The creation of a new phrase UFSAR-described…" could be understood to be different in meaning that the previously defined term.

Commented [A7]: CONSISTENT with PRIOR COMMENT: see Comment No. 5.

1 The term, "design function," as used throughout this document, has the meaning as defined in NEI 96-07 Revision 1, Section 3.3 (on page No. 12).

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.

Examples 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.

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

Commented [A8]: NEW SUGGESTION: The first sentence was added because it provides additional context.

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.

Commented [A9]: CONSISTENT with PRIOR COMMENT: see Comment No. 5.

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

In other words, the examples cited above are not changes that fundamentally alter (replace) the existing means of performing or controlling design functions as described in NEI 96-07, Section 4.2.1.2.

Therefore, engineering/technical information should be documented (as part of the design process) to demonstrate that there are no adverse impacts from the above activities.

Scope of Digital Modifications

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

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 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

(c) Dependability Impact

USE OF SOFTWARE AND DIGITAL DEVICES

The UFSAR may identify SSC design function conditions such as diversity, separation, independence, defense-in-depth and/or redundancy through UFSAR discussions. With digital modifications, software and/or hardware have the potential to impact design function conditions such as the diversity,

Commented [A10]: COMMENT: The phrase "In other words" is incorrect and the sentence is otherwise misleading because NEI 96-07, Section 4.2.1.2 is not even applicable to the examples.

Commented [A11]: SUGGESTED CHANGE: Suggest the deletion of concept of "design function condition," because it is unnecessary. Furthermore, its use here is inconsistent with NEI 96-07.

Diversity … are design requirements or design attributes, not conditions as described in NEI 96-07. Furthermore, reductions in … require a LAR per NEI 96-07 Section 4.3.2 which states:
"Examples 5-8 are cases that would require prior NRC approval because they would result in more than a minimal increase in the likelihood of occurrence of a malfunction of an SSC important to safety: ...Example 6
The change would reduce system/equipment redundancy, diversity, separation or independence."

"Design functions" and associated "conditions" are defined in NEI 96-07, Section 3.3. The definition of "conditions" is not consistent with labeling "diversity…" as conditions.

This correction in terminology should be made throughout.

separation, independence, defense-in-depth, and/or redundancy of SSCs explicitly and/or implicitly described in the UFSAR.[2]

To assist in determining the impact of a digital modification on design function conditions such as the diversity, separation, independence, defense-in-depth and/or redundancy of the affected SSCs, compare the proposed features of the affected SSCs with the existing features of the affected SSCs. The impact of any differences in the diversity, separation, independence, defense-in-depth and/or redundancy on design functions described in the UFSAR is then determined.

A digital modification that reduces existing SSC diversity, separation, independence, defense-in-depth and/or redundancy is *adverse*.[3]

In addition, an adverse effect may also consist of the potential marginal increase (i.e., in an adverse direction) 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 further consideration of a software common cause failure. In such cases, even when a digital modification involves redundant systems, the digital modification would be *not adverse*.~~

In some cases, a licensee's UFSAR may describe diversity and defense-in-depth; both of which address~~, in part, software~~ CCF. Engineering evaluations of design attributes should not be used to relax conformance to such diversity and defense-in-depth requirements when performing a 50.59 screen. Any relaxation of conformance to such diversity and defense-in-depth requirements is *adverse*.

Alternately, the use of different software in two or more redundant SSCs is *not adverse* due to a software ~~common cause failure~~CCF because there is no mechanism to increase the likelihood of failure due to the introduction of software.

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

[2] Refer to NEI 96-07, Section 4.2.1.1, 2nd paragraph.

[3] NEI 96-07 Section 4.3.2 states:
"Examples 5-8 are cases that would require prior NRC approval because they would result in more than a minimal increase in the likelihood of occurrence of a malfunction of an SSC important to safety: ...Example 6
The change would reduce system/equipment redundancy, diversity, separation or independence."

Commented [A12]: NEW SUGGESTION: As stated in NEI 96-07.

Commented [A13]: NEW SUGGESTION: A footnote was added below in the following paragraph to support this clarification.

Commented [A14]: NEW SUGGESTION: For added clarity.

Commented [A15]: SUGGESTED CHANGE: This paragraphs could be moved into the "Dependability Impact" subsection below because it discuss "reliability" which in more related to dependability than the five design attributes of this section.

Commented [A16]: NEW: The paragraph was deleted because it is not correct for screening; therefore corrections suggested by NEI in a comment were not incorporated.

Commented [A17]: CONSISTENT with PRIOR COMMENT: Diversity and defense-in-depth address all types of CCF, not just software CCF.

Commented [A18]: SUGGESTED CHANGE: The last two sentences of this paragraph do not provide any additional guidance above that of NEI 96-07 and can be deleted.

Commented [A19]: EDITORIAL: see Comment No. 4

- Addition or removal of a dead-band, or
- Replacement of instantaneous readings with time-averaged readings (or vice-versa).

Example 4-1 illustrates ~~when~~ that a reduction in ~~diversity or~~ independence is adverse.

Commented [A20]: EDITORIAL: The example does not talk about a reduction in diversity.

Example 4-1. 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.

Design Function Identification

A design function condition of separation is identified since two physically separate analog control systems are described in the UFSAR.

Commented [A21]: SUGGESTED CHANGE: Suggest deletion of the concept of "design function condition," in this example, per Comment No. 11.

A design function condition of independence is identified since the UFSAR states that the two analog control systems have no common controls, inputs or components.

Commented [A22]: SUGGESTED CHANGE: Suggest deletion of the concept of "design function condition," in this example because it is unnecessary. (see Comment No. 5.)

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

Screen Response

(a) Redundancy Consideration: There is no impact on redundancy since there are no design function conditions related to redundancy.

(b) Diversity Consideration: There is no impact on diversity since there are no design function conditions related to diversity.

(c) Separation Consideration: There is no impact on the separation of the control systems identified in the design function conditions since each of the analog control systems will be replaced with a separate digital control system.

(d) Independence Consideration: The independence of the two control systems is impacted now that the exact same software will be installed in both digital control systems.

(e) Defense-in-Depth Consideration: There is no impact on defense-in-depth

since there are no design function conditions related to defense-in-depth.

Through consideration of ONLY items (a) through (e) above, there is an *adverse* impact on the method of performing or controlling the design function of the main feedwater control system due to the use of common software in both digital devices which reduces the independence of the two control systems.

~~For some relatively simple digital modifications, engineering evaluations may show that the risk of failure due to software is not significant and need not be evaluated further, even in applications of high safety significance. In such cases, e~~Even when a digital modification involves redundant systems, the digital modification may not be adverse. ~~The engineering evaluation will have concluded that the digital system is sufficiently dependable, based on considerations.~~ To screen out relatively simple digital modifications, the degree of assurance needed to conclude that change does not have an adverse effect on a design function is based on considerations such as:

- The quality of the design processes employed
- The change has a limited scope (e.g., replace analog transmitter with a digital transmitter that drives an existing instrument loop)
- Single failures of the digital device are bounded by existing failures of the analog device (e.g., no new digital communications among devices that introduce possible new failure modes involving separate devices).
- 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 are used to drive signals for parameters monitored),
- Can be comprehensively tested (but not necessarily 100 percent of all combinations); and,
- Has extensive applicable operating history.

Commented [A23]: UNDELETED & EDITED: This paragraph and the following bullets were deleted by NEI after the Direct Edits meeting. NRC recommends this be kept in and un-deleted the text.

Track changes is used to show changes to the un-deleted text.

If NEI believes they need to remove this guidance, then further discussion would be required.

COMBINATION OF COMPONENTS/SYSTEMS AND/OR FUNCTIONS

The UFSAR may identify the number of components/systems, how the components/systems were arranged, and/or how functions were allocated to those components/systems. Any or all of these characteristics may have been considered in the process of identifying possible malfunctions or accident initiators.

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 for any reason can potentially affect multiple 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 a reduction in the required or assumed SSC design function conditions such as diversity, separation, independence, defense-in-depth and/or redundancy or in an SSC's ability or capability to perform a design function (e.g., by the creation of a new malfunction or the creation of a new malfunction or accident initiator) is the combination aspect of the digital modification *adverse*.

Of particular interest when combining components/systems and/or functions using digital devices is the combination of previously completely separate components and/or systems that were not physically or electrically related (or "coupled") in any manner. An example of this type of combination would be the combination of the feedwater control system and the main turbine control system into one ~~digital control device~~segment of a distributed control system. In this case, the failure of the single ~~digital device~~segment consisting of both control systems causes the failure of both feedwater control and turbine control, which is *adverse*.

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 and/or design function conditions.

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

- Combining previously separate functions into one digital device such that failures create new malfunctions (i.e., multiple functions are disabled if the digital device fails).
- Changing performance from UFSAR-described requirements (e.g., for response time, accuracy, etc.).
- Changing functionality in a way that increases complexity, potentially creating new malfunctions.
- Introducing different behavior or potential failure modes that could affect the design function.

Commented [A24]: SUGGESTED CHANGE: Suggest deletion of the concept of "design function condition," per Comment No. 11.

Commented [A25]: SUGGESTED CHANGE: Suggest deletion of the concept of "design function condition," because it is unnecessary. (see Comment No. 5.)

Commented [A26]: SUGGESTED CHANGE: Since NEI 96-07 clearly establishes that any reduction in … requires a LAR, it seems redundant to say that combinations that result in … screen in.

Therefore the guidance in the section was changed to address new failures or malfunctions directly rather than via a reduction in ….

Commented [A27]: COMMENT: This text is clarified by the inserted paragraph and bullets below.

Commented [A28]: NEW SUGGESTION: NRC suggest this change to provide clarity on the example. The same principle is demonstrated by the suggested edits.

Commented [A29]: CONSISTENT with PRIOR COMMENT: This block of inserted text comes from NEI 01-01 Section 4.3.3, "Other digital Issues in the Screening Process."

The NRC formally asked that this text be inserted in the NRC formal Screening comments (ML17068A092 Comment No. 14).

Examples 4-2 and 4-3 illustrate the application of the *Combination of Components/Systems and/or Functions* aspect.

Examples 4-2a and 4-2b illustrate how variations in a proposed activity can affect the Screen conclusion.

Example 4-2a. Combining Components and Functions with ~~NO~~ ADVERSE IMPACT on a Design Function

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. System drawings ~~(incorporated by reference into the UFSAR)~~ show that each analog control system has many subcomponents.

Within each control system loop 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 and functions in each analog control system loop 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.

Design Function Identification

A design function condition of separation is identified since two physically separate analog control systems are described in the UFSAR.

A design function condition of independence is identified since the UFSAR states that the two analog control systems have no common controls, inputs or components.

Although the control systems and the major components are described in the UFSAR, only a design function for the feedwater control system is identified. ~~No design functions for any of the individual components are described in the UFSAR.~~ 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 all feedwater to the steam generators, and

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

Screen Response

NOTE: Since the intent of this example is to illustrate the combination aspect ONLY, the software and hardware aspects will be

Commented [A30]: CONSISTENT with PRIOR COMMENT: Whether the it is described in or referenced by the UFSAR is not a relevant criteria.

Suggest deletion per Comment No. 5.

Commented [A31]: CONSISTENT with PRIOR COMMENT: Whether the it is described in or referenced by the UFSAR is not a relevant criteria.

Suggest deletion per Comment No. 5.

Commented [A32]: SUGGESTED CHANGE: This sentence can be deleted because it introduces the concept of "independence" (per example 4-1) which is not mentioned in the conclusion.

Furthermore, because of Example 4-1 above, this change would fail the "independence" criteria.

Commented [A33]: SUGGESTED CHANGE: per Comment No. 11.

Commented [A34]: CONSISTENT with PRIOR COMMENT: This sentence adds unnecessary (and potentially confusing) information. It does not matter if the design function is described in the UFSAR. The inclusion of this sentence implies that it has an impact on the conclusion, which is misleading.

ignored.

(a) Redundancy Consideration: There is no impact on redundancy since there are no design function conditions related to redundancy.

(b) Diversity Consideration: There is no impact on diversity since there are no design function conditions related to diversity.

(c) Separation Consideration: There is no impact on the separation of the two control systems since the combination of components and functions involves only the components and functions within one loop.

(d) Independence Consideration: There is no impact on the independence of the two control systems, due to the combination aspects only (i.e., excluding consideration of the same software, which is addressed in Example 4-1), since the combination of components and functions involves only the components and functions within one loop.

(e) Defense-in-Depth Consideration: There is no impact on defense-in-depth since there are no design function conditions related to defense-in-depth.

Through consideration of ONLY items (a) through (e) above, there is *no adverse* impact on the method of performing or controlling 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 and functions in each of the two loops.

~~Through consideration of~~ However, the MFWP control system ~~malfunctions~~ modification ~~that have already been considered, the combination of components and functions~~ has an ~~no~~ *adverse* impact because previously separate functions were combined into one digital device such that failures of the digital device create new malfunctions (i.e., multiple functions are disabled if the digital device fails) and introduces different behavior or potential failure modes. ~~on the identified design function because no new malfunctions are created.~~

Using the same initial SSC configuration, proposed activity, design function and design function conditions information and malfunctions from Example 4-2a, Example 4-2b illustrates how a variation in the proposed activity would be addressed.

Example 4-2b. Combining Components and Functions with an ADVERSE IMPACT on a Design Function

Instead of two separate, discreet, unconnected digital control systems being used for the feedwater control systems, only one central digital processor is proposed to be used that will combine the previously separate control systems

Commented [A35]: SUGGESTED CHANGE: The focus should be on the creation of new failures or malfunctions as stated in the 3rd introductory paragraph of this sub-section.

Commented [A36]: EDITORIAL: Please compare with the position in 4-1 above.

This example needs to be understood to say that the combination aspect alone does not make the modification adverse, although other aspects do.

Commented [A37]: CONSISTENT with PRIOR COMMENT: This concluding paragraph is changed to match the changed guidance above.

The concept being that ANY new malfunction should screen. The evaluation section would then determine whether the new malfunction exceeds the evaluation criteria.

and control both feedwater pumps.

In this case, the proposed activity is *adverse* because there is a reduction in the separation and independence of the two original control systems due to the combination aspect.

Example 4-3 illustrates the combining of control systems from different, originally separate systems.

Example 4-3. 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

A design function condition of separation of each feedwater control system is identified since two physically separate analog control systems are described in the UFSAR.

A design function condition of separation of the feedwater control systems and the main turbine steam inlet valve control system is identified since three physically separate analog control systems are described in the UFSAR.

A design function condition of independence is identified since the UFSAR states that the two feedwater control analog control systems and the main turbine steam inlet valve control system have no common controls, inputs or components.

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 identify 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

(a) Redundancy Consideration: There is no impact on redundancy since there

Commented [A38]: SUGGESTED CHANGE: Suggest deletion of the concept of "design function condition," in this example, per Comment No. 11.

Commented [A39]: SUGGESTED CHANGE: Suggest deletion of the concept of "design function condition," in this example because it is unnecessary. (see Comment No. 5.)

are no design function conditions related to redundancy.

(b) Diversity Consideration: There is no impact on diversity since there are no design function conditions related to diversity.

(c) Separation Consideration: There is an impact on the separation of the two feedwater control systems from the main turbine control system since the combination of components and functions involves eliminating the separation of these three control systems.

(d) Independence Consideration: There is an impact on the independence of the two feedwater control systems from the main turbine control system since the combination of components and functions involves eliminating the independence of these control systems.

(e) Defense-in-Depth Consideration: There is no impact on defense-in-depth since there are no design function conditions related to defense-in-depth.

Through consideration of ONLY items (a) through (e) above, there are *adverse* impacts on the method of performing or controlling 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.

Through consideration of the feedwater and main turbine control system malfunctions that have already been considered, the combination of components and functions has an *adverse* impact on the identified design functions because a possible new malfunction has been created.

Commented [A40]: COMMENT: This paragraph in combination with the following one implies that "new malfunctions" are only considered adverse if they impact "separation" or "independence." While the guidance above uses 'or' which means either one results in an adverse determination.

DEPENDABILITY IMPACT

In the main body of NEI 96-07, Section 4.2.1, subsection titled "Screening for Adverse Effects," reliability is mentioned in the following excerpt:

> "...*a change that decreases* /(i.e., in an adverse direction)/ *the reliability of a function whose failure could initiate an accident would be considered to adversely affect a design function*..."

Commented [A41]: NEW SUGGESTION: Clarifies.

Based on engineering evaluations, the Screen should assess the dependability of performing design functions due to the introduction of software and/or hardware.[4]

Commented [A42]: NEW SUGGESTION: Clarifies

4 NEI 96-07 Section 4.2.1, page No. 32, states:
"If a change has both positive and adverse effects, the change should be screened in. ... The screening process is not concerned with the magnitude of adverse effects that are identified."

Examples 4-4b and 4-4c illustrate the application of the guidance for a digital modification.

Example 4-4b. NO ADVERSE IMPACT on a Design Function for a 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 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 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. This process runs in a continuous sequence with no branching or interrupts.

Failures of the new digital device are bounded 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 sufficiently dependable, 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 two outputs), 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 reliability of performing the design function is not reduced~~.

Note that an upgrade that is similar to Example 4-4b, but that uses digital communications from the smart transmitter to other components in the instrument loop might screen in because new interactions and potentially new failure behaviors are introduced that could have adverse effects and should be analyzed in a 10 CFR 50.59 evaluation ~~(see Example 4-B)~~.

Commented [A43]: NEW SUGGESTION: The guidance immediately above provides criteria for "adverse' or not, and does not mention reliability.

Furthermore, the next example below, also does not mention reliability.

Commented [A44]: UNDELETED & EDITED: This paragraph was deleted by NEI after the direct edit meeting. NRC recommends keeping it and undeleted it. Track changes shows any subsequent changes.

Example 4-4c. Screening for a Smart Transmitter (Screens In)

Smart transmitters similar to those described in Example 4-4b are to be installed as part of an upgrade to the reactor protection system. The new smart transmitters have the capability to transmit their output signal using a digital communication protocol. Other instruments in the loop are to be replaced with units that can communicate with the transmitter using the same protocol. Because this change not only upgrades to a digital transmitter but also converts the instrument loop to digital communications among devices, there would be the potential for adverse effects owing to the digital communication and possible new failure modes involving multiple devices.

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

As a result of the adverse effect on a design function, this change screens in.

Commented [A45]: UNDELETED & EDITED: This was example 4-B. After the direct edits meeting NEI deleted this example. NRC recommends keeping it and reinserted it and made changes as shown.

4.2.1.2 Screening of Changes to Procedures as Described in the UFSAR

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.

There are three "basic HSI elements" of an HSI (Reference: NUREG-0700):

- **Displays:** the visual representation of the information operators 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.

Operators (and any other users 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).

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 ~~each of the four~~ generic primary tasks that are "involved" (i.e. potentially impacted by the modification) with the proposed activity.

- Step Two - For ~~each~~ all primary tasks involved, assess ~~how~~ if the modification may negatively impact~~impacts (i.e., *positively or negatively)*~~ 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 i~~nvolve~~s the standard Screen assessment process (i.e., identification of design functions and determination of *adverse* or *not adverse*, including the justification for the conclusion).

Commented [A46]: HFE/HSI COMMENT
COMMENT on IMPLEMENTATION: The following wording is different than NRC revision. Although the wording is different, if NEI is willing to accept the minor in-text revisions made here, the NRC is OK with this text.

NRC version:
To determine potential adverse effects of HSI modifications on design functions, a four-step analysis must be performed. Step one is identifying whether any/all of the four generic primary tasks are potentially impacted by the modification. Step two involves assessing how the modification might negatively impact the operators' abilities to perform any/all of the four generic primary tasks. Step three consists of identifying the design functions relevant to the proposed modification. Step four consists of determining if the impacts identified in step two result in adverse effects on the relevant UFSAR-described design function(s) identified in step three.
Examples of negative impacts on operator 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,*
- *creation of new potential failure modes.*

Table 1 contains examples of modifications to each of the three basic HSI elements ~~that should be addressed in the response to~~ applicable to this Screen consideration.

Commented [A47]: NEW SUGGESTION: To improve clarity.

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)

~~Examples 4-5a through 4-5c illustrate the application of the HSI assessment process outlined above. In Examples 4-5a through 4-5c, certain HSI elements (i.e., "displays" and "user interface...") will be deliberately ignored to focus on the "controls" HSI element.~~

SIMPLE EXAMPLE

Assessment of Modification with NO ADVERSE IMPACT on a UFSAR-Described Design Function

Proposed Activity Description:

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.

HSI ASSESSMENT PROCESS

STEP 1. Identification of the Generic Primary Tasks Involved:

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

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

As part of the technical evaluation supporting the proposed modification, a human factors evaluation was performed (For full details see document XXX). Task 4 was identified as involved; the human factors 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, this UFSAR description implicitly identifies the SSC (i.e., the knob) and the design function of the SSC (i.e., its ability to allow the operator to manually adjust the position of the flow control valve).

Commented [A48]: HFE/HSI COMMENT
COMMENT on IMPLEMENTATION: The below Examples 4-5 through 4-7 are not agreed upon examples.

The simple example agreed upon deals with a modification as a whole. In other words, it does not try to focus on one aspect of a modification and ignore other aspects.

What is proposed here are examples that "certain HSI elements (i.e., "displays" and "user interface...") will be deliberately ignored to focus on the "controls" HSI element." This applies to examples 4-5a-4-7. The process the NRC proposed is based upon the tenet that a comprehensive HSI evaluation is necessary to determine the impacts of HSI modifications. That comprehensive process is lost when providing piece-meal examples.

If NEI believe they need to add these HSI examples, additional review time and meetings would have to be planned.

Using the results from the human factors 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.

Based on this assessment, this modification should SCREEN OUT because the modification does not adversely impact the relevant FSAR design functions.

~~Example 4-5a. HSI Modification Emphasizing the "Controls" Element with NO ADVERSE IMPACT on a Design Function~~

~~Proposed Activity Description~~

~~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. The knob contains a tactile feedback feature that, as it is being rotated through each setting increment, informs the operator that an adjustment is occurring.~~

~~The knob will be replaced with a touch screen that has two separate arrows, each in its own function block. Using the touch screen, touching the "up" arrow will open the flow control valve in 1% increments and touching the "down" arrow will close the flow control valve in 1% increments. The tactile feedback feature cannot be incorporated into the touch screen, so that feature will not be retained.~~

~~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) – 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 the Modification Impacts on the Generic Primary Tasks~~

~~As part of the engineering evaluation supporting the proposed modification, a human factors engineering (HFE) evaluation was performed.~~

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

modification.

Task 4 was involved. The HFE evaluation determined that the change from a knob to a touch screen did not have any impact on the operator because there was no change to the ability of the operator to perform the task.

Identification and Assessment of Design Functions

Design Function Identification

The design function states the operator can "open and close the flow control valve using manual controls located in the Main Control Room."

Screen Response

Using the results from the HFE evaluation, the replacement of the knob with a touch screen is *not adverse* since the ability of the operator to "open and close the flow control valve using manual controls located in the Main Control Room" is not affected and is maintained.

1

Example 4-5b. HSI Modification Emphasizing the "Controls" Element with an ADVERSE IMPACT on a Design Function

Proposed Activity Description

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. The knob contains a tactile feedback feature that, as it is being rotated through each setting increment, informs the operator that an adjustment is occurring.

The knob will be replaced with a touch screen that has two separate arrows, each in its own function block. Using the touch screen, touching the "up" arrow will open the flow control valve in 1% increments and touching the "down" arrow will close the flow control valve in 1% increments. The tactile feedback feature cannot be incorporated into the touch screen, so that feature will not be retained.

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 Generic Primary Tasks

As part of the engineering evaluation supporting the proposed modification, a human factors engineering (HFE) evaluation was performed.

Task 1 was involved. The HFE evaluation determined that the elimination of the tactile feedback feature has a negative impact on the operator because the ability of the operator to recognize when the setting has changed has been eliminated.

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

Task 4 was involved. The HFE evaluation determined that the change from a knob to a touch screen did not have any impact on the operator because there was no change to the ability of the operator to perform the task.

Identification and Assessment of Design Functions

Design Function Identification

The design functions identify that the operator can "open and close the flow control valve using manual controls located in the Main Control Room," and that "the control mechanism provides tactile feedback to the operator as the mechanism is rotated through each setting increment as a means of informing the operator that an adjustment is occurring."

Screen Response

Using the results from the HFE evaluation, the replacement of the knob with a touch screen is *not adverse* since the ability of the operator to "open and close the flow control valve using manual controls located in the Main Control Room" is not affected and is maintained.

Using the results from the HFE evaluation, elimination of the tactile feedback feature is *adverse* because the "means of informing the operator that an adjustment is occurring" will no longer be satisfied.

1

Example 4-5c. HSI Modification Emphasizing the "Controls" Element with an ADVERSE IMPACT on a Design Function

Proposed Activity Description

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. The knob contains a tactile feedback feature that, as it is being rotated through each setting increment, informs the operator that an adjustment is occurring

The 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.

In addition to the touch screen control arrows themselves, a sound feature and associated components will be added to the digital design that will emit a clearly audible and distinct "tone" each time the control setting passes through the same setting increment that the tactile feature provided with the mechanical device.

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 Generic Primary Tasks

As part of the engineering evaluation supporting the proposed modification, a human factors engineering (HFE) evaluation was performed.

Task 1 was involved. The HFE evaluation determined that, although the change from tactile feedback to auditory feedback meant that a form of feedback still existed, the change from tactile feedback to auditory feedback has a negative impact on the operator because a new potential failure mode has been created (e.g., using auditory feedback, high ambient sound levels could prevent the operator from hearing the auditory feedback).

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

Task 4 was involved. The HFE evaluation determined that the change from a knob to a touch screen did not have any impact on the operator because there was no change to the ability of the operator to perform the task.

Identification and Assessment of Design Functions

Design Function Identification

The design functions identify that the operator can "open and close the flow control valve using manual controls located in the Main Control Room," and that "the control mechanism provides tactile feedback to the operator as the mechanism is rotated through each setting increment as a means of informing the operator that an adjustment is occurring."

Screen Response

Using the results from the HFE evaluation, the replacement of the knob with a touch screen is *not adverse* since the ability of the operator to "open and close the flow control valve using manual controls located in the Main Control Room" is not affected and is maintained.

Although the replacement of the tactile feedback feature with an auditory feedback feature retains the feedback feature, the creation of a new potential failure is *adverse* because the reliability of performing the design function has been reduced.

In Example 4-6, the "controls" and "user interface..." HSI elements will be deliberately ignored to focus on the "displays" HSI element.

Example 4-6. HSI Modification Emphasizing the "Displays" Element with NO ADVERSE IMPACT on a Design Function

Proposed Activity Description

Currently, all controls and indications for a single safety-related pump are analog. There are two redundant channels of indications, either of which can be used to monitor pump performance, but only one control device. For direct monitoring of pump performance, redundant *motor electrical current* indicators exist. For indirect monitoring of pump performance, redundant *discharge pressure* and *flow rate* indicators exist. Furthermore, at the destination of the pump's flow, redundant *temperature* indicators exist to allow indirect monitoring of pump performance to validate proper pump operation by determination of an increasing temperature trend (i.e., indicating insufficient flow) or a stable/decreasing temperature trend (i.e., indicating sufficient flow).

A digital system will replace all of the analog controls and indicators. Two monitoring stations will be provided, either of which can be used to monitor the pump. Each monitoring station will display the information from one of the two redundant channels. The new digital system provides the ability to monitor each of the performance indications and inform/alert the operator of the need to take action.

HSI Assessment Process

Step 1: Identification of Which Four Generic Primary Tasks are Impacted

(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) - NOT INVOLVED
(4) Response implementation (performing an action) - NOT INVOLVED

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

As part of the engineering evaluation supporting the proposed modification, a human factors engineering (HFE) evaluation was performed.

Task 1 was involved. The HFE evaluation determined that there is no impact on the operator because the same amount and type of information will be available with the digital systems as existed with the analog systems. 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.

Task 2 was involved. The HFE evaluation determined that there is no impact on the operator because the same set of pump performance parameters will be available with the digital systems as existed with the analog systems.

Tasks 3 and 4 were not involved, so this task is not impacted by the modification.

Identification and Assessment of Design Functions

Design Function Identification

The design function states that "the information necessary to perform this task is one parameter directly associated with the pump (motor electrical current) and three parameters indirectly associated with pump performance (discharge pressure, flow rate, and response of redundant temperature indications)."

Screen Response

The HFE evaluation has determined that the new digital systems provide the same number (one) and type (motor electrical current) of pump parameters to directly ascertain pump performance and that the new digital systems provide the same number (three) and type (discharge pressure, flow

rate and redundant temperature) of system parameters to indirectly ascertain pump performance. Since the same number and type of parameters are still available, there is *no adverse* impact on the design functions to perform direct and indirect monitoring of pump performance.

In Example 4-7, the "displays" and "controls" HSI elements will be deliberately ignored to focus on the "user interface..." HSI element.

Example 4-7. HSI Modification Emphasizing the "User Interface..." Element with an ADVERSE IMPACT on a Design Function

Proposed Activity Description

Currently, two redundant channels/trains of information are provided to the operators in the Main Control Room for a specific safety-related system. 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. No control functions are included within the scope of this digital modification.

A digital modification consolidates the system information onto two flat panel displays (one for each redundant channel/train). The HSI flat panel displays will present the information layout by "flow path" to reflect the current arrangement (identified as the *primary* view) and by "channel/train" (identified as the *alternate* view) to allow comparison of each individual component value/status.

In addition, the digital systems provide many other display options to the user (e.g., individual component status and component/system alarms), all of which are collectively identified as *supporting* views.

The flat panels normally display the *primary* view arrangement that mimics the analog display arrangement. If a flat panel display is not manually returned to the *primary* view from any of the other displays, the digital system will automatically return the display to the *primary* view after 30 seconds unless halted or delayed by the user using the **Halt/Delay Return** control button on each display. If the **Delay** option is selected, the user is prompted to enter the delay time (in minutes). Anytime the **Halt/Delay Return** button is used, returning the display to the *primary* view must be performed manually using the **Primary View** button.

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) - NOT INVOLVED
(4) Response implementation (performing an action) - NOT INVOLVED

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

As part of the engineering evaluation supporting the proposed modification, a human factors engineering (HFE) evaluation was performed.

Tasks 1 and 2 are involved. With the new displays and display options available to the operators, the operators can choose which parameters to display and how that information is displayed (e.g., by train/path, etc.). The HFE evaluation concluded that this modification could result in the operator not having 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.

Tasks 3 and 4 were not involved, so these tasks are not impacted by the modification.

Identification and Assessment of Design Functions

Design Function Identification

(a) The operator can "examine system performance and utilize the information from at least one of the redundant system channels to verify performance."

(b) The physical layout of the instrumentation and indications is by "flow path" to allow the operator to determine overall system performance.

Screen Response

Based on the HFE evaluation results that demonstrate that the tasks can still be performed, there are *no adverse* impacts on design function (a) since this design function will continue to be satisfied.

The information available and the organization of that information in the new displays is *selectable* based on operator preference. Critical status indications may not be displayed when needed, thus there is an *adverse* impact on design function (b).

COMPREHENSIVE HUMAN-SYSTEM INTERFACE EXAMPLES

No additional guidance is provided in this section. Examples 4-8a and 4-8b illustrate how a digital modification with ~~extensive~~ 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 ~~Extensive~~ 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, which ~~can~~ displays the information ~~for only one train~~ and the controls for only that train, replicating the information and controls arrangement as they are in the existing HSI.

The 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

Commented [A49]: **HFE/HSI COMMENT**
COMMENT on IMPLEMENTATION: This section contains the examples provided by the NRC with some modifications made by NEI.

Commented [A50]: **HFE/HSI COMMENT**
COMMENT on IMPLEMENTATION: This is not "extensive" but rather a "typical" HSI modification. This title sets an expectation that most HSI-related modifications will be simpler, and this is not correct.

Commented [A51]: **HFE/HSI COMMENT**
COMMENT on IMPLEMENTATION: This is not "extensive" but rather a "typical" HSI modification. This title sets an expectation that most HSI-related modifications will be simpler, and this is not correct.

Commented [A52]: **EDITORIAL:**

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 human factors 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.

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.

Commented [A53]: **COMMENT on IMPLEMENTATION:** You only have to assess the tasks involved.

Commented [A54]: **COMMENT on IMPLEMENTATION:** Not needed since tasks are not involved.

Commented [A55]: **HFE/HSI COMMENT**
COMMENT: This is not consistent with NRC example. "The operator must be able to switch from the automatic mode to manual mode. Second, the control switch must be turned to the start position."

This design function was pulled directly from an actual UFSAR.

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).

Although the modification increases the difficulty and amount of time needed for an operator to manipulate a control, 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).

Based on this assessment, this modification should SCREEN OUT because the modification does not adversely impact the identified design functions.

Commented [A56]: HFE/HSI COMMENT
COMMENT on IMPLEMENTATION: A final screening statement is needed for clarity.
(i.e., To summarize the previous two paragraphs)

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

Commented [A57]: HFE/HSI COMMENT
NEW SUGGESTION: This is not "extensive" but rather a "typical" HSI modification. This title sets an expectation that most HSI-related modifications will be simpler, and this is not correct.

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:

Commented [A58]: COMMENT on IMPLEMENTATION: You only have to assess the tasks involved.

As part of the technical evaluation supporting the proposed modification, a human factors 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, etc.). 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~~ may negatively impact the operator's understanding of how the information relates to system performance. This negative impact on understanding ~~will~~ may also negatively impact the operator's ability to assess the situation and plan an appropriate response.

Commented [A59]: NEW SUGGESTION: To be more correct.

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.

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).~~

Since, t~~T~~he information available and the organization of that information in the new displays is *customizable* based on operator preference, ~~.~~ c ~~C~~ritical status indications may not be continuously available to the operator, thus there is an *adverse* impact on design function (a).

Although the modification increases the difficulty and amount of time needed for an operator to manipulate a control, 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).

Based on this assessment, this modification should SCREEN IN because the modification adversely impacts a design function.

Commented [A60]: EDITORIAL: Old paragraph was not deleted, as was probably intended.

Commented [A61]: EDITORIAL:

Commented [A62]: EDITORIAL:

Commented [A63]: **NEW SUGGESTION:** To summarize the previous two paragraphs.

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~~s~~ Focus

Examples are provided to illustrate the guidance provided herein. 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 that, if considered, could potentially change the Evaluation conclusion.

Many of the examples in this section involve the Main Feedwater (MFW) System to illustrate concepts. The reason for selecting the MFW system is that it is one of the non-safety-related systems that, upon failure, can initiate an accident. Furthermore, a failure of the MFW system is one of the malfunctions that is also an accident initiator.

Qualitative Assessment

For digital I&C systems, reasonable assurance of low likelihood of failure is derived from a qualitative assessment of factors involving system design features, the quality of the design processes employed, and the operating history 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.

~~Common Cause Failure (~~Software CCF~~)~~ Likelihood Determination Outcomes

The possible outcomes of a~~n engineering evaluation~~ qualitative assessment~~(e.g., from a CCF Susceptibility Analysis)~~, performed in accordance with applicable Industry and/or NRC guidance documents, that determined software CCF likelihood, are as follows:

(1) Software CCF likelihood is **sufficiently low** (as defined in Definition 3.15), or

(2) Software CCF likelihood is **not sufficiently low**.

These outcomes will be used in developing the responses to Evaluation criteria 1, 2, 5 and 6.

Human-System Interface Evaluations

Similar to other technical evaluations (performed as part of the design modification package), the HFE determines what the outcomes of the change will be (e.g., personnel acts or omissions, as well as their likelihoods and effects). The evaluations performed under 50.59 compare the new outcomes (i.e., post modification) to the old outcomes (i.e., pre-modification) in order to determine whether a license amendment is required.

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

INTRODUCTION

From NEI 96-07, Section 3.2:

Commented [A64]: SUGGESTED CHANGE: This paragraph is not needed. NRC staff suggests deletion of this paragraph, because it does not provide guidance.

In justifying the choice of examples, it makes the implicit argument that the examples are not adequate (i.e., they need justification).

Commented [A65]: NEW SUGGESTION: Previously this was in the definition section, and it is discussed and found unacceptable as a definition in the Direct Edits meeting. However, NRC staff finds it is appropriate here to provide clarification on the use of a qualitative assessment and recommends this be added.

Related to Comment No.

Commented [A66]: CONSISTENT with PRIOR COMMENT: In September, it was agreed to replace CCF Susceptibility Analysis with Qualitative assessment. (see Comment No. 4)

Commented [A67]: HFE/HSI COMMENT
NEW SUGGESTION: This text is being added by NRC staff as a ways of saying that no specific HFE guidance is needed for licensing.

"*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.

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 software CCF, which will be addressed in this section's guidance. An example of a potential source of CCF that is not unique to digital is consideration of the impact on accident frequency due to the digital system's compatibility with the environment in which the system is being installed, 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 section's 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 ~~in the UFSAR~~, then there is no attributable impact on the frequency of occurrence of an accident.

Commented [A68]: HFE/HSI COMMENT
NEW SUGGESTION: HSI guidance is not based on whether it is digital or not.

Commented [A69]: HFE/HSI COMMENT
NEW: Wording changed to address the following scenario?

A digital modification is planned for a non-safety display which is not associated with an accident initiator in the UFSAR. My understanding is that the conclusion would be that there is no attributable impact on the frequency or occurrence of an accident.

Does it matter that the operator may look at the modified display and come to a (perhaps erroneous) conclusion that he must take action using safety related controls which are not necessarily a part of the current modification and that may have predictable impacts on the frequency or occurrence of an accident?

The conclusion drawn by the operator may be erroneous, especially if there is an unrecognized corruption of data on the updated display, but the accident may be initiated using non-modified equipment.

Is there a part of the process that evaluates this sort of interaction between the human and system?

Commented [A70]: CONSISTENT with PRIOR COMMENT: The UFSAR only contains the "limiting" accidents, however, for this criteria, all accidents must be considered.

Deleted, see Comment No. 5.

Alternately, if any component/system involved with the digital modification is identified as an accident initiator ~~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 [A71]: CONSISTENT with PRIOR COMMENT: The UFSAR only contains the "limiting" accidents, however, for this criteria, all accidents must be considered.

Deleted, see Comment No. 5.

Commented [A72]: CONSISTENT with PRIOR COMMENT: The UFSAR only contains the "limiting" accidents, however, for this criteria, all accidents must be considered.

Deleted, see Comment No. 5.

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, a~~n examination~~ qualitative assessment of all the factors associated with the digital modification and their interdependent relationship need to be considered and addressed as part of the response to this Evaluation criterion~~, as identified below:~~.

~~A. SCCF Factor~~

An engineering evaluation of the design and the design process determines the likelihood of failure due to software via a common cause failure. The engineering evaluation that assesses CCF likelihood will identify if the CCF likelihood is **sufficiently low** or the CCF likelihood is **not sufficiently low.**

B. Non-SCCF Factors

1. Use of Software

Software developed in accordance with a defined life cycle process, and that complies with applicable industry standards and regulatory guidance does not inherently result in more than a minimal increase in the frequency of an accident. The design process and the design documentation contain the information that will be used to determine if software increases the frequency of occurrence of an accident.

2. Use of Digital Components (e.g., microprocessors in place of mechanical devices)

NOTE: This factor is not unique to digital and would be addressed by applying the guidance described in NEI 96-07, Section 4.3.1. This factor is included here for completeness.

Digital components are expected to be more reliable than the equipment being replaced. Aspects to be addressed include the following: compliance with applicable regulations and industry standards; qualification for environmental conditions (e.g., seismic, temperature, humidity, radiation, pressure, and electromagnetic compatibility); performance requirements for the plant-specific application; proper design of electrical power supplies; cooling or ventilation for thermal loads; and separation, independence and grounding. The design process and the design documentation contain the information that will be used to determine if the use of digital components increases the frequency of occurrence of an accident.

3. Intended Benefits of the Digital Component/System

NOTE: This factor is not unique to digital and would be addressed by applying the guidance described in NEI 96-07, Section 4.3.1. This factor is included here for completeness.

In addition to the expected hardware-related reliability improvements of the physical devices themselves (addressed in factor 2 above), overall improvements in the reliability of the performance of the digital component/system, operational flexibility and/or maintenance-related activities may also be achieved. The design documentation contains the information that will be used to identify the intended benefits of

~~the digital component/system and possible impacts on the frequency of occurrence of an accident.~~

~~4. Design Attributes/Features~~

~~Design attributes of the proposed digital modification are features that serve to prevent or limit failures from occurring, or that mitigate the results/outcomes of such possible failures. Factors to be considered include the following items:~~

- ~~Design Criteria (as applicable) (e.g., diversity, independence and redundancy)~~
- ~~Inherent Design Features for Software, Hardware or the Architectural/Network (e.g., watchdog timers that operate independent of software, isolation devices, segmentation, self-testing and self-diagnostic features)~~
- ~~Non-concurrent Triggers~~
- ~~Software Architecture Complexity (i.e., enabling comprehensive, but not necessarily 100%, testing)~~
- ~~Unlikely Series of Events (e.g., the evaluation of a given digital modification would need to postulate multiple independent random failures in order to arrive at a state in which a SCCF is possible)~~
- ~~Failure State (e.g., always known to be acceptable)~~

Negligible:

To achieve a *negligible* conclusion, the examination of all the factors would conclude that the ~~not~~ 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)***," [5] [***emphasis*** added] due to the ~~not~~ effect of the factors considered, ~~(i.e., use of software, use of digital components, intended benefits and design attributes/features)~~ **AND** the software CCF likelihood is **sufficiently low**.

Discernable:

If the examination of all the factors concludes that the ~~not~~ 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 CCF likelihood could be **sufficiently low** or **not sufficiently low**. ~~However, to remain consistent with the guidance provided in NEI 96-07, Section 4.3.1, a *discernable* increase in the accident frequency may NOT be~~

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

Commented [A73]: NEW: NRC staff deleted the word "net." To be consistent with wording in NEI 96-07.

Reliability is like a chain, it is the weakest link that determines behavior. It does not really matter how good the other links are.

Commented [A74]: COMMENT on IMPLEMENTATION: Per Comment A8 (of the redline version provided for this November meeting -Rev. 0d), NRC & NEI agreed to put the qualitative assessment guidance in a separate document, and that no "partial" guidance would be provided in this document.

Commented [A75]: NEW: To be consistent with wording in NEI 96-07.

~~more than minimal if applicable NRC requirements, as well as design, material, and construction standards, to which the licensee is committed, continue to be met.~~ Furthermore, NEI 96-07, Section 4.3.1, states:

> "Although this criterion allows minimal increases, licensees must still meet applicable regulatory requirements and other acceptance criteria to which they are committed (such as contained in regulatory guides and nationally recognized industry consensus standards, e.g., the ASME B&PV Code and IEEE standards). Further, departures from the design, fabrication, construction, testing and performance standards as outlined in the General Design Criteria (Appendix A to Part 50) are not compatible with a "no more than minimal increase" standard."

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

~~Factors Considered:~~

~~A. SCCF Factor - CCF likelihood is **sufficiently low**.~~

~~B. Non-SCCF Factors~~

~~1. Software - Developed in accordance with a defined life cycle process, and complies with applicable industry standards and regulatory guidance~~

~~2. Digital Components - More reliable, comply with all applicable standards, and meet all applicable technical requirements~~

~~3. Benefits - Reliability and performance increased~~

Commented [A76]: CONSISTENT with PRIOR COMMENT: Changed wording to be consistent with NEI 96-07.

PREFERABLY, all this wording can be deleted since it is in NEI 96-07.

~~4. Design Attributes/Features~~

- ~~Design Criteria - Independence and redundancy are maintained~~
- ~~Inherent Design Features for Software, Hardware or the Architectural/Network - Watchdog timers that operate independently of software, isolation devices, segmentation, self-testing and self-diagnostic features exist~~
- ~~Non-concurrent Triggers - Verified~~
- ~~Software Architecture Complexity - Comprehensive testing~~
- ~~Unlikely Series of Events - Multiple independent random failures are not possible~~
- ~~Failure State - All states are known to be acceptable~~

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 ~~not~~ change in the frequency of occurrence of the Loss of Feedwater event is *negligible* due to the ~~not~~ 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.

Commented [A77]: COMMENT on IMPLEMENTATION: Per Comment A8 (of the redline version provided for this November meeting -Rev. 0d), NRC & NEI agreed to put the qualitative assessment guidance in a separate document, and that no "partial" guidance would be provided in this document.

Related to Comment No. 74

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

~~Factors Considered:~~

~~A. SCCF Factor - CCF likelihood is **not sufficiently low**.~~

~~B. Non-SCCF Factors~~

~~1. Software - Same as Example 4-11.~~

~~2. Digital Components - Same as Example 4-11.~~

~~3. Benefits - Same as Example 4-11.~~

~~4. Design Attributes/Features - Same as Example 4-11.~~

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 ~~not~~ change in the frequency of occurrence of the Loss of Feedwater event is *discernable* due to the ~~not~~ effect of the factors considered in the qualitative assessment.

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, consideration of the net effect of all the non-SCCF factors, the satisfaction of applicable requirements and other acceptance criteria to which the licensee is committed, as well as applicable design, material and~~ additional~~construction standards, there is NOT more than a minimal increase in the frequency of occurrence of the accident due to the digital modification.~~

HUMAN-SYSTEM INTERFACE ASSESSMENT

If no personnel-based initiators (i.e., 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.

If personnel-based initiators (e.g., operator error) are identified among the accident initiators, then 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 [A78]: COMMENT on IMPLEMENTATION: Per Comment A8 (of the redline version provided for this November meeting -Rev. 0d), NRC & NEI agreed to put the qualitative assessment guidance in a separate document, and that no "partial" guidance would be provided in this document.

Related to Comment No. 74

Commented [A79]: CONSISTENT with PRIOR COMMENT: It is implied that these other factors mitigate the effects of the increase in frequency of occurrence due to a SW CCF. This does not seem like a logical conclusion; NRC staff deleted this text to resolve the confusion.

Related to Comment No. 76

Commented [A80]: HFE/HSI COMMENT
NEW SUGGESTION: Suggest replacing (e.g., operator error) with (i.e., degraded operator performance) to reinforce a broader focus than operator error.

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 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 softwareCCF, which will be addressed in this section's guidance. An example of a potential source of CCF 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 section's guidance.

GUIDANCE

As discussed in NEI 96-07, Section 4.3.2, Example 6, a proposed activity that reduces redundancy, diversity, separation or independence of design function conditions is considered more than a minimal increase in the likelihood of 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. (NOTE:

Commented [A81]: EDITORIAL: There are many places in this section where the words are identical to the previous section. The words in this section should be updated after agreement is reached on the associated words in the previous section.

Alternatively, this document would be shorter if there was not so much duplication. This wording could be stated once in Section 4.3.

The phrase "credited in the safety analyses" is discussed in NEI 96-07, Section 3.3.)

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 a malfunction initiator 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 a malfunction initiator 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 occurrence of a malfunction.

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

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 Malfunctions and Malfunction Initiators

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.

Impact on Malfunction Likelihood

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 previously considered, 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.)

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

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 examination of all the factors associated with the digital modification and their interdependent relationship need to be considered and addressed as part of the response to this Evaluation criterion, as identified below:

A. SCCF Factor

An engineering evaluation of the design and the design process determines the likelihood of failure due to software via a common cause failure. The engineering evaluation that assesses CCF likelihood will identify if the CCF likelihood is **sufficiently low** or the CCF likelihood is **not sufficiently low**.

B. Non-SCCF Factors

1. Use of Software

Software developed in accordance with a defined life cycle process, and that complies with applicable industry standards and regulatory guidance does not inherently result in more than a minimal increase in the likelihood of a malfunction. The design process and the design documentation contain the information that will be used to determine if software increases the likelihood of occurrence of a malfunction.

2. Use of Digital Components (e.g., microprocessors in place of mechanical devices)

NOTE: This factor is not unique to digital and would be addressed by applying the guidance described in NEI 96-07, Section 4.3.2. This factor is included here for completeness.

Digital components are expected to be more reliable than the equipment being replaced. Aspects to be addressed include the following: compliance with applicable regulations and industry standards; qualification for environmental conditions (e.g., seismic, temperature, humidity, radiation, pressure, and electromagnetic compatibility); performance requirements for the plant-specific application; proper design of electrical power supplies; cooling or ventilation for thermal loads; and separation, independence and grounding. The design process and the design documentation contain the information that will be used to determine if the use of digital components increases the likelihood of occurrence of a malfunction.

3. Intended Benefits of the Digital Component/System

NOTE: This factor is not unique to digital and would be addressed by applying the guidance described in NEI 96-07, Section 4.3.2. This factor is included here for completeness.

In addition to the expected hardware-related reliability improvements of the physical devices themselves (addressed in factor 2 above), overall improvements in the reliability of the performance of the digital component/system, operational flexibility and/or maintenance-related activities may also be achieved. The design documentation contains the information that will be used to identify the intended benefits of the digital component/system and possible impacts on the likelihood of occurrence of a malfunction.

4. Design Attributes/Features

Design attributes of the proposed digital modification are features that serve to prevent or limit failures from occurring, or that mitigate the results/outcomes of such possible failures. Factors to be considered include the following items:

- Design Criteria (as applicable) (e.g., diversity, independence and redundancy)
- Inherent Design Features for Software, Hardware or the Architectural/Network (e.g., watchdog timers that operate independently of software, isolation devices, segmentation, self-testing and self-diagnostic features)
- Non-concurrent Triggers
- Software Architecture Complexity (i.e., enabling comprehensive, but not necessarily 100%, testing)

- Unlikely Series of Events (e.g., the evaluation of a given digital modification would need to postulate multiple independent random failures in order to arrive at a state in which a SCCF is possible)
- Failure State (e.g., always known to be acceptable)

Negligible:

To achieve a *negligible* conclusion, the examination of all the factors would conclude that the net 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* ***no clear trend toward increasing the likelihood)***"[6] [***emphasis*** added] due to the net effect of the factors considered (i.e., use of software, use of digital components, intended benefits and design attributes/features) **AND** the CCF likelihood is **sufficiently low**.

Discernable:

If the examination of all the factors concludes that the net 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 CCF likelihood could be **sufficiently low** or **not sufficiently low**. However, to remain consistent with the guidance provided in NEI 96-07, Section 4.3.2, a *discernable* increase in the malfunction likelihood may NOT be more than minimal if applicable NRC requirements, as well as design, material, and construction standards, to which the licensee is committed, continue to be met.

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

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

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

Factors Considered:

A. SCCF Factor - CCF likelihood is **sufficiently low**.

B. Non-SCCF Factors

1. Software - Developed in accordance with a defined life cycle process, and complies with applicable industry standards and regulatory guidance

2. Digital Components - More reliable, comply with all applicable standards, and meet all applicable technical requirements

3. Benefits - Reliability and performance increased

4. Design Attributes/Features

- Design Criteria - Independence and redundancy are maintained
- Inherent Design Features for Software, Hardware or the Architectural/Network - Watchdog timers that operate independently of software, isolation devices, segmentation, self-testing and self-diagnostic features exist
- Non-concurrent Triggers - Verified
- Software Architecture Complexity - Comprehensive testing
- Unlikely Series of Events - Multiple independent random failures are not possible
- Failure State - All states are known to be acceptable

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 net 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 net effect of the factors considered.

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 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

Factors Considered:

A. SCCF Factor - CCF likelihood is **not sufficiently low**.

B. Non-SCCF Factors

1. Software - Developed in accordance with a defined life cycle process, and complies with applicable industry standards and regulatory guidance

2. Digital Components - More reliable, comply with all applicable standards, and meet all applicable technical requirements

3. Benefits - Reliability and performance increased

4. Design Attributes/Features

- Design Criteria - Independence is NOT maintained
- Inherent Design Features for Software, Hardware or the Architectural/Network - Watchdog timers that operate independently of software, isolation devices, segmentation, self-testing and self-diagnostic features exist
- Non-concurrent Triggers - Verified
- Software Architecture Complexity - Comprehensive testing
- Unlikely Series of Events - Multiple independent random failures are not possible
- Failure State - All states are known to be acceptable

The net change in the likelihood of occurrence of the malfunction of both safety injection pumps is *discernable* due to the net effect of the factors considered. 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 CCF being **not sufficiently low**, which does not satisfy single failure criteria. 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 (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.

If personnel-based initiators (e.g., operator error) are identified among the malfunction initiators, then 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 *credible* 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 Credible

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.).*"

Hence, "credible" accidents are defined as those as likely as the accidents already assumed in the UFSAR.

If the software CCF likelihood is determined to be **sufficiently low**, then the creation of a possibility for an accident of a different type is NOT *credible*.

If the software CCF likelihood is determined to be **not sufficiently low**, then the creation of a possibility for an accident of a different type is *credible*.

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 credible, 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[7], or

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

Accidents of a different type are credible accidents 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

7 In this case Question No. 6 is applicable.

Commented [A82]: COMMENT: This material may not needed. Most of it already exist in the base document.

The one sentence summary confuses the content of the two sentences. That is, there are two sentences in the quotation, and they address two criteria (one for each sentence). The first sentence addresses likelihood, while the second addresses assumptions.

Commented [A83]: NEW SUGGESTED: Since many events meet the definition of both "accident" and "malfunction," a note could be added to say that revisions are also evaluated under question (vi).

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

Credible Conclusion

Based on an engineering evaluation and the failure modes and effects analysis (FMEA) performed as part of the technical assessment supporting this digital modification, the likelihood of a software CCF causing the loss of both feedwater control systems (resulting in the loss of both MWFPs) 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 *credible* and there is no need to determine the accident analysis impact.

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

Credible Conclusion

Based on an engineering evaluation and the failure modes and effects analysis (FMEA) performed as part of the technical assessment supporting this digital modification, the likelihood of a software CCF 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 *credible* 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) through (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 do 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.

Commented [A84]: SUGGESTED CHANGE: Since many events meet the definition of both "accident" and "malfunction," a note could be added to say that revisions are also evaluated under question (vi).

Related to Comment No. 83

HUMAN-SYSTEM INTERFACE ASSESSMENT

If no personnel-based initiators (i.e., degraded operator performance) are affected by the NEW accident initiators, then the NEW accident cannot occur due to the Human-System Interface portion of the digital modification.

Commented [A85]: HFE/HSI COMMENT
NEW SUGGESTION: NRC staff suggests adding this HFE guidance for completeness.

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

[LATER]

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]