NEI PROPOSED REVISIONS
(Document Date: May 16, 2017)

NEI 96-07, Appendix D
Draft Revision 0c

Nuclear Energy Institute

SUPPLEMENTAL GUIDANCE FOR APPLICATION OF 10 CFR 50.59 TO DIGITAL MODIFICATIONS

NEI PROPOSED REVISIONS
(Document Date: May 16, 2017)

May 2017

NEI PROPOSED REVISIONS
(Document Date: May 16, 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

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.

TABLE OF CONTENTS

EXECUTIVE SUMMARY .... **i**

1 INTRODUCTION **2**

1.1 BACKGROUND 2432

1.2 PURPOSE 354332

2 [NOT USED]DEFENSE IN DEPTH DESIGN PHILOSOPHY AS APPLIED TO DIGITAL I&C465443

3 DEFINITIONS AND APPLICABILITY OF TERMS **476643**

4 IMPLEMENTATION GUIDANCE **798873**

4.1 APPLICABILITY 7109973

4.2 SCREENING 81110974

4.3 EVALUATION PROCESS 363634332723

5.0 EXAMPLES **707167675852**

1 INTRODUCTION

~~The intent of the § 50.59 process is to permit licensees to make changes to the facility, provided the changes maintain the level of safety documented in the original licensing basis, such as in the safety analysis report.~~ 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~~ing, for example,~~ different potential failure modes of digital equipment as opposed to the equipment being replaced, the effect of combining functions of previously separate devices into one device, and the potential for software common cause failure (software CCF).

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 ~~proposed~~ stated that NEI could separate~~ing~~ technical guidance from 10 CFR 50.59 related guidance.

Commented [A1]: Source: ML17170A089 Comment No. A2
Rationale: To improve accuracy: NEI first proposed this idea, and then the NRC documented that is had no objection.

~~EPRI document 3002005326, *Methods for Assuring Safety and Dependability when Applying Digital Instrumentation and Control Systems,*~~

~~has been created to provide technical guidance for the development and design of digital systems with the purpose of systematically identifying, assessing, and managing failure susceptibilities of I&C systems and components. However, the use of EPRI 3002005326 is not required for the application of the 50.59-related guidance in this appendix.~~

~~NEI 16-16, *Guidance for Addressing Digital Common Cause Failure* has been created to provide technical guidance for addressing Common Cause Failure (CCF) for compliance to deterministic licensing criteria and NRC policies and positions such as SRM-SECY-93-087 and BTP 7-19. The technical-focused guidance contained in NEI 16-16, used in conjunction with the licensing-focused guidance in this document, provides a complimentary set of approaches and considerations when implementing a digital modification. However, the use of NEI 16-16 is not required for the application of the 50.59-related guidance in this appendix.~~

Commented [A2]: Not necessary for 50.59 guidance.

1.2 PURPOSE

Appendix D is intended to assist licensees in the performance of 10 CFR 50.59 reviews of activities involving digital modifications in a consistent and comprehensive manner. This assistance includes guidance for performing 10 CFR 50.59 Screens and 10 CFR 50.59 Evaluations. This appendix does not include guidance regarding design requirements for digital activities.

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

Commented [A3]: This clarification is needed since the guidance in this document only includes aspects unique to digital equipment.

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

~~This section is not used for digital modifications.~~No additional guidance is provided.

1.5 CONTENT OF THIS GUIDANCE DOCUMENT

~~This section is not used for digital modifications.~~ No additional guidance is provided.

2 ~~[NOT USED]~~DEFENSE IN DEPTH DESIGN PHILOSOPY AS APPLIED TO DIGITAL I&C

~~This section is not used for digital modifications.~~No additional guidance is provided.

3 DEFINITIONS AND APPLICABILITY OF TERMS

~~There are no definitions or modifications to the definitions necessary for application of 10 CFR 50.59 to digital modifications~~ Definitions 3.1 through 3.14 are the same as those provided in NEI 96-07, Rev. 1. Terms specific to this ~~document~~ appendix are defined below.

~~3.1 10 CFR 50.59 EVALUATIONS~~

~~No additional giuidance is provided.~~

~~3.2 ACCIDENTS PREVIOUSLY EVALUATED IN THE UFSAR (AS UPDATED)~~

~~No additional giuidance is provided.~~

Commented [A4]: Source: ML13298A787 Issue Nos. 5, 7, 9, & 10
Rationale: As discussed in the "sources," 50.59 implementers have had trouble distinguishing between technical criteria and 50.59 criteria. The basic problem was they used guidance for one to do the other.

Commented [A5]: Source: ML13298A787 Issue Nos. 5, 7, 9, & 10
Text adapted from NEI 01-01 Section 5.2
Rationale: It is necessary to clearly articulate the D3 criteria, and show they are not new, but have always been there. It has been the application of these criteria to a new technology (i.e., digital I&C) that has been confusing to industry; therefore the basic concepts must be stated and agreed to.

Commented [A6]: Source:
(1) ML17068A092 Comment No. 12
(2) ML17170A089 Comment No. A4
Rationale: New terms are defined since undefined terms are a source of regulatory uncertainty.

3.3 Change

No additional giuidance is provided.

3.4 Deprture from a method of evaluation Decribed in the UFSAR

No additional giuidance is provided.

3.5 Design Bases (Design Basis)

No additional giuidance is provided.

3.6 Facility as Described in the UFSAR

No additional giuidance is provided.

3.7 Final Safety Analysis Report (as updated)

No additional giuidance is provided.

3.8 Input Parameters

No additional giuidance is provided.

3.9 Malfunction of a SSC Important to Safety

No additional giuidance is provided.

3.10 Methods of Evaluation

No additional giuidance is provided.

3.11 Procedures as described in the UFSAR

No additional giuidance is provided.

3.12 Safety Analysis

No additional giuidance is provided.

~~3.13 SCREENING~~

~~No additional giuidance is provided.~~

~~3.14 TEST OR EXPERIMENTS NOT DESCRIBED IN THE UFSAR~~

~~No additional giuidance is provided.~~

3.15 CCF

[LATER - coordinate with NEI 16-16]

3.16 SOFTWARE CCF

[LATER - coordinate with NEI 16-16]

~~3.17 CCF SUSCEPTABILITY ANALYIS~~

Commented [A7]: Source:
(1) ML17068A092 Comment No. 12
(2) ML17170A089 Comment No. A4, A28, & A29
Rationale: New terms should be defined since undefined terms are a source of regulatory uncertainty.

~~3.18 PLANT LEVEL EFFECTS~~

~~3.19 Qualitative Assessment~~

Commented [A8]: Global change to be addressed during meeting: Any examples that refer to technical information that is part of the qualitative assessment should state that the design satisfies the "suffently low" likelihood of the qualitative assessment instead of describing a select incomplete piece.

~~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.~~

[REMOVE USE OF THE TERM "QUALITATIVE ASSESSMENT"]

3.17 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, calibration errors).

4 IMPLEMENTATION GUIDANCE

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

In general, since digital systems can not be verified to contain no errors, two separate aspects should be considered, the design process and the design. A high quality design process is used to minimize the likelihood of errors in the softeware, and the design is evaluated to ensure it contains the proper design attributes to ensure the assumptions of the accident analysis are maintained.

Design Process: For digital upgrades one of the challenges in the 10 CFR 50.59 process is addressing the effect of software, and potential failures of software, on a UFSAR-described design function. The answer lies in the engineering evaluations that are performed throughout the design process.

Design: Another challenge is evaluating the effect that design changes to system architecture has on the assumptions in the accident analyses, such as, diversity, defense-in-depth, and independence. Furthermore, the coupling or combining of functions and/or equipment also has the potential to challenge these same assumptions.
[Verify addressed in Screen and Evaluation sections]

4.1 APPLICABILITY

There is no Applicability guidance unique to digital modifications.Section 4.1 of NEI 96-07, Revision 1, provides guidance on the applicability of 10 CFR 50.59. In some cases, a change may be controlled by more specific regulations. Also, for digital-to-digital changes that appear to be like-for-like replacements, an equivalency evaluation should be performed to determine in

Commented [A9]: Source: NEI 01-01 Page No 4-7.
Reason: To provide context. Small changes made to improve clarity.

Commented [A10]: Source: ML17170A089 Comment No. A37
Rationale: Sotware development proceses and software design are two distinct things, and each should be addressed separately.

This background material and the following two paragraphs support other changes in the evaluation section.

Commented [A11]: Source: NEI 01-01 Section 4.1
Reason: To provide context. Small changes made to improve clarity.

Commented [A12]: Source: Engineering judgement
Reason: To provide context.

~~the replacement is a plant design change (subject to 10 CFR 50.59) versus a maintenance activity. Digital-to-digital change may not necessarily be like-for-like because the system behaviours, respionse time, failure modes, etc. for the new system may be different from the old system. If the vendor, hardware, firmware, application software, and the configuration data are identical, then the upgrade may be a like-for-like maintenance activity where 10 CFR 50.59 would apply.~~

Commented [A13]: Source: NEI 01-01 Section 4.2
Reason: To provide missing guidance.

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.

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

In NEI 96-07, Section 4.2.1.1, equivalent replacements are discussed. Digital-to-digital changes may not necessarily be equivalent because the system behaviours, response time, failure modes, etc. for the new system may be different from the old system.

As stated in NEI 96-07, Section 4.2.1, the determination of the impact of a proposed activity (i.e., *adverse* or *not adverse*) is based on the impact of the proposed activity on UFSAR-described design functions. To assist in determining the impact of a digital modification on a UFSAR-described design function, the general guidance from NEI 96-07 will be supplemented with the digital-specific guidance in the topic areas identified below.

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.

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 that, if considered, could potentially change the Screen conclusion.

~~The first step in screening is to determine whether the change affects a design function as described in the UFSAR. If it does not, then the change screens out, and can be implemented without further evaluation under the 10 CFR 50.59 process. If the change does affect a UFSAR-described design function, then it should be evaluated to determine if it has an adverse affect. Changes with adverse effects areas those that have the potential to increase the likelihood of malfunctions, increase consequences, create new accidents, or otherwise meet the 10 CFR 50.59 evaluation criteria. Additional guidance on the definition of adverse is provided in the bulleted examples below:~~

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

~~As discussed in 4.2.1, "Is the Activity a Change to the Facility or Procedures as Described in the UFSAR?," Aa given activity may have both direct and indirect effects that the screening review must consider. Consistent with historical practice, changes to the facility or procedures affecting SSCs or functions not described in the UFSAR must be screened for their effects (so-called "indirect effects") on UFSAR-described design functions. A 10 CFR 50.59 evaluation is required when such changes adversely affect a UFSAR-described design function.~~

~~Examples 4-C and 4-D illustrate typical screening considerations for a small digital upgrade.~~

~~***Example 4-C. Screening for a Recorder Upgrade (Screens Out)***~~

~~An analog recorder is to be replaced with a new microprocessor based recorder. The recorder is used for various purposes including Post Accident Monitoring, which is an UFSAR-described design function. An engineering/technical evaluation performed on the change determined that~~

Commented [A14]: Global Comment: Do not mention "described in the UFSAR" when indirect effects must be considered because it incorrectly implies that whether something is explicitly described UFSAR is a factor in 50.59 decisionmaking. Specifically, explicitly described in the UFSAR is not a factor in screening (e.g., HSI) or criterion 2. NEI 96-07r1 clearly states when explict UFSAR wording matters (e.g., UFSAR described "design functions, "accidents", "methods of evaluation")

Commented [A15]: Source: NEI 01-01 Section 4.3.3
Reason: To provide guidance. the following 2 examples are from NEI 01-01.

Commented [A16]: Source: ML17006A341 Comment No. A2
Reason: To provide example to illustrate when digital modifications are or are not adverse.

~~the new recorder will be highly dependable (based on a quality development process, testability, and successful operating history) and therefore, the risk of failure of the recorder due to software is considered very low. The new recorder also meets all current required performance, HSI, and qualification requirements, and would have no new failure modes or effects at the level of the design function. The operator will use the new recorder in the same way the old one was used, and the same information is provided to support the Post Accident Monitoring function, so the method of controlling or performing the design function is unaltered. The licensee concludes that the change will not adversely affect any design function and screens out the change.~~

~~***Example 4-D. Screening for a Recorder Upgrade (Screens In)***~~

~~Similar to Example 4-C, a licensee is planning to replace an analog recorder with a new microprocessor based recorder. However, in this instance, the engineering/technical evaluation determined that the new recorder does not truly record continuously. Instead, it samples at a rate of 10 hertz then averages the 10 samples and records the average every one second. This frequency response is lower compared to the originalequipment and may result in not capturing all process variable spikes or short-lived transients. In this case, the licensee concludes that there could be an adverse effect on an UFSAR-described design function and screens in the change. In the 10 CFR 50.59 evaluation, the licensee will evaluate the magnitude of this adverse effect.~~

Commented [A17]: Source: ML17006A341 Comment No. A2
Reason: To provide example to illustrate when digital modifications are or are not adverse.

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

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

Although there may be ~~the potential for the introduction of~~ 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 (i.e., not a change that fundamentally alters (replaces) the existing means of performing or controlling design function as described in NEI 96-07, Section 4.2.1.2), for example:

- 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.

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

> **Commented [PM18]:** Placeholder for NRC comment A18

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.

> **Commented [PM19]:** Placeholder for NRC comment A19
> **Formatted:** Highlight
> **Formatted:** Highlight

> **Commented [PM20]:** Placeholder for NRC comment A20
> **Formatted:** Highlight
> **Formatted:** Highlight

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

SCOPE

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 ~~few~~ non-safety-related systems that, upon failure, can initiate an accident.

> **Commented [A21]:** **Source:** ML170170A089 Comment No. A6.
> **Rationale:** Based on the definition of "accident" in NEI 96-07, many accidents are initiated by non-safety related SSCs. (Note: safety related SSCs are tpicaly credited to miigate accidents.)

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/Functions

(c) Dependability Impact

Examples of activities that have the potential to cause an adverse effect include the following activities:

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

USE OF SOFTWARE AND DIGITAL DEVICES

The UFSAR may identify SSC design function conditions such as~~through~~ 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, separation, independence, defense-in-depth, and/or redundancy of SSCs explicitly and/or implicitly described in the UFSAR.[1]

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~~ described in the UFSAR, identify the features of the affected SSCs described in the UFSAR.~~, ~~C~~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 ~~the~~ design functions described in the UFSAR ~~of the affected SSCs~~ is then determined.

A digital modification that reduces SSC diversity, separation, independence, defense-in-depth and/or redundancy is *adverse*. In addition, an adverse effect may also consist of the potential marginal increase in the likelihood of SSC failure due to the introduction of software. For redundant safety systems, this marginal increase in likelihood creates a similar marginal increase in the likelihood of a common failure in the redundant safety systems. On this basis, most digital modifications to redundant safety systems are *adverse*. ~~However, for some digital modifications, engineering evaluations, using methods approved by the NRC, may show that the digital modification contains design attributes to eliminate consideration of a software common cause failure. In such cases, even when a digital modification involves redundant systems, the digital modification would be *not adverse*.~~ Note:

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

Commented [A22]: Strickly speaking "diversity, separation, independence, defense-in-depth and/or redundancy" are properties or attributes of a design and not "design functions;" however, NEI 96-07 page 12 states: "Implicitly included within the eaning of design function are the conditions under which intened functions are required to be performed, such as equipment response times, process conditions, equipment qualification and single failure." Therefore "diversity, separation, independence, defense-in-depth and/or redundancy" can be considered conditions of design functions.

Alternatively, the first sentence of this paragraph could be deleted.

Commented [A23]: Imporantly, adverse impact due to software is not limited to factors related to the diversity, separation, independence, defense-in-depth, and/or redundancy.

Commented [A24]: Source:
(1) ML17068A092 Comment No. 9
(2) ML17170A089 Comment No. A8
Rationale: An SSC does not need to be described in the FASR (as updated) for a change to it to adversely affect a FSAR (as updated)-described design function.

Commented [A25]: Source: None
Rationale: To improve claity. This intent being that only after it is determined that there is no reduction in … then one can consider …

As previously written, someone could have understood that design atribtes can allow for reductions in diversity, separation, independence, defense-in-depth and/or redundancy.

Commented [A26]: Consider replacing with qualitative assessment guidance from RIS.

~~In some cases the regulations require, and/or the UFSAR includes: (1) diversity, and (2) defense-in-depth; both of which address, in part, 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 screening and evaluation.~~

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, even when a digital modification involves redundant systems, the digital modification would be *not adverse*. The engineering evaluation will have concluded that the digital system is sufficiently dependable, 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 operating history.

Considerations for screening relatively simple digital equipment are illustrated in Example 4-A.

Example 4-A. Screening for a Smart Transmitter (Screens Out)

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 limit scope in that for each channel, the existing 4-20 mA instrument loop is maintained 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. The digital transmitters use a relatively simple digital architecture internally in that the firmware in the new transmitters implements a simple process of acquiring one input signal, setting one output, and performing some simple diagnostic checks. This process runs in a continuous sequence with no branching or interrupts.

Single failures of the digital device are bounded by existing failures of the analog device in that no new digital communications among devices that introduce possible new failure modes involving multiple devices. A "qualitative assessment" of the digital device concluded that the digital system is sufficiently dependable, 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.

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

Consequently, it is concluded that no adverse effects on UFSAR-described design functions are created, and the change screens out.

Note that an upgrade that is similar to Example 4-A, 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).

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

Smart transmitters similar to those described in Example 4-A 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 affect on a UFSAR-described design function, this change screens in.

In some cases, the licensee's UFSAR describes (1) diversity, and (2) 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.

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

Examples 4-1a and 4-1b illustrate the application of the *Use of Software and Digital Devices* aspect. These examples illustrate how a variation in the licensing basis identified in the UFSAR can affect the Screen conclusion.

Example 4-1a. NO ADVERSE IMPACT on a UFSAR-Described Design Function related to use of Software and Digital Devices

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.

The pertinent UFSAR SSC descriptions are as follows:

(1) Two analog control systems are identified.

(2) Both analog control systems consist of the same physical and functional characteristics.

(3) The analog control system malfunctions include (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.

The pertinent UFSAR-described design function of the main feedwater system is to automatically control and regulate feedwater to the steam generators.

With respect to the following considerations, the ~~U~~use of the same hardware platforms and same software in both control systems is NOT ADVERSE ~~for the following reasons~~:

(a) Redundancy Consideration: There is no impact on redundancy since ~~the UFSAR does not describe redundant SSCs and~~ there are no UFSAR-described design function conditions related to redundancy.

(b) Diversity Consideration: There is no impact on diversity since ~~the UFSAR does not describe diverse SSCs and~~ there are no UFSAR-described design function conditions related to diversity.

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

(d) Independence Consideration: Although both of the new digital control systems contain the exact same software (which is subject to a software common cause failure), the Failure Modes and Effects Analysis (FMEA) performed as part of the technical assessment supporting the digital modification concluded that no new types of malfunctions are introduced since the loss of both MFWPs and failures causing an increase in main feedwater flow to the maximum output from both MFWPs are already considered in the licensing basis.

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

Commented [PM27]: Placeholder to align original comment numbering.

Commented [A28]: Source:
(1) ML17068A092 Comment No. 9
(2) ML17170A089 Comment No. A11
Rationale: It does not mater if it is described in the FSAR (as updated) or not.

Commented [A29]: Source: ML17170A089 Comment No. A12
Rationale: It does not mater if it is described in the FSAR (as updated) or not.

since ~~the UFSAR does not describe SSCs for the purpose of establishing defense-in-depth and~~ there are no UFSAR-described design function conditions related to defense-in-depth.

Through consideration of items (a) through (e) above, there is NO ADVERSE impact on the method of performing or controlling the design function of the main feedwater system to automatically control and regulate feedwater to the steam generators due to the use of software and digital devices.

Example 4-1b. ADVERSE IMPACT on a UFSAR-Described Design Function related to use of Software and Digital Devices

This example differs from Example 4-1a in only the types of malfunctions already identified in the UFSAR, as reflected in item (3) shown below.

Items (1) and (2) are unaffected.

(3) [Modified from Example 4-1a] The analog control system malfunctions include (a) failures causing the loss of feedwater from only ***one*** MWFP to the steam generators and (b) failures causing an increase in main feedwater flow to the maximum output from only ***one*** MFWP.

The use of the same hardware platforms and same software in both control systems is ADVERSE due to its impact on the Independence Consideration.

Items (a), (b), (c) and (e) are unaffected.

(d) [Modified from Example 4-1a] Independence Consideration: Since the new digital control systems contain the exact same software (which is subject to a software common cause failure), the Failure Modes and Effects Analysis (FMEA) performed as part of the technical assessment supporting the digital modification concluded that two new types of malfunctions are introduced since the loss of ***both*** MFWPs and failures causing an increase in main feedwater flow to the maximum output from ***both*** MFWP have been created and were not considered in the original licensing basis.

There is an ADVERSE impact on the design function of the main feedwater system to automatically control and regulate feedwater to the steam generators due to the use of software that reduces independence and creates two new types of malfunctions.

Commented [A30]: Source: ML17170A089 Comment No. A13
Rationale: It does not mater if it is described in the FSAR (as updated) or not.

Commented [A31]: Source:
(1) ML17068A092 Comment No. 4
(2) ML17170A089 Comment No. A14
Rationale: NEU 96-07 Rev. 1 Section 3.3 defines "Method of performing of controlling a function" and it is used exclusively to refer to the things people do.

COMBINATION OF COMPONENTS/FUNCTIONS

The UFSAR may identify the number of components, how the components were arranged, and/or how functions were allocated to those components. 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 and/or functions into a single device or control system. However, the failure of the single device or control system for any reason ~~(e.g., a software common cause failure)~~ can potentially affect multiple functions.

The combination of previously separate components and/or functions ~~(that does not reduce SSC design aspects such as diversity, separation, independence, defense-in-depth and/or redundancy)~~, in and of itself, does not make the Screen conclusion adverse. Only if combining the previously separate components and/or functions causes a reduction in ~~one of these aspects or a reduction in~~ ~~athe~~ the required or assumed SSC design aspects such as diversity, separation, independence, defense-in-depth and/or redundancy or in an SSC's ability or capability ~~of~~ to performi~~ng~~ 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.

To assure ~~adequate~~ existing defense in depth is maintained, one should first identify potential coupling factors between equipment failures. A coupling factor is the condition or mechanism through which multiple components could be affected (or coupled) by the same cause. [*DISCUSS MORE LATER, IN CONJUCTION WITH EXAMPLE 4-A AND 4-B*]

~~To assist in determining the impact of a digital modification on the number and/or arrangement of components, review the description(s) of the existing SSCs described in the UFSAR (as updated).~~ When comparing the existing and proposed configurations, consider how the proposed configuration affects the number and/or arrangement of components and the potential impacts of the proposed arrangement on UFSAR-described design functions.

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

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

Commented [A32]: Source: ML13298A787 - Concerns 5 & 7
Rationale: Presumably this section was added to address this concern.

Commented [A33]: Single device failures or misbehaviours are by definition not CCFs. Only when there are multiple components that are assumed to be independent can one call it a CCF; therefore this example is technically incorrect.

Commented [A34]: Source: In several meetings, Industry expressed that "not all combinations are bad."
Rationale: These word help provide conceptual guidance for distinguishing combinations that are of regulatory concern, from those that do not.
The combinations that are bad are the one that combine or couple items that span these criteria.

Commented [A35]: As screening criteria, ANY reduction in one of these aspects should be considered adverse. Whether the outcomes of such a reduction requires a LAR, is the subject of the evaluation section.

Commented [A36]: Source: ML17170A089 Comment No. A16
Rationale: Change includes indirect effects.

Commented [A37]: Source:
(1) ML17006A341 Comment No. A2
(2) ML170170A089 Comment No. A10.
(3) Text adapted from DG-1285 (ML16358A153)
(4) ML13298A787 - Concern 10
Rationale: To add key aspects to consider when determining whether a digital modification should be considered adverse (or not) for 50.59 screening purposes.

Commented [A38]: As written this sentence is ambigious. Without this change, it could be interpreted that only FSAR described arrangements (as opposed to actual arrangements) matter. The criteria should be actual arangements, whether described in the FSAR or not.

Alternatively the entire first sentence could be deleted.

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

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.

All of the analog subcomponents will be replaced with a single digital device that consolidates all of the components, sub-components and the technical functions associated with each component and sub-component. 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 pertinent UFSAR SSC descriptions are as follows:

(1) Two analog feedwater control systems are identified, including several major individual components.

(2) The SSC descriptions state that both analog control systems consist of the same physical and functional characteristics.

Although the control systems and the major components are described in the UFSAR, only a UFSAR-described design function for the feedwater control system is identified. No design functions for any of the individual components are described in the UFSAR. The pertinent UFSAR-described design function of the feedwater control system is "to provide adequate cooling water to the steam generators during normal operation."

The UFSAR identifies the following MFWP control system malfunctions:

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

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

The combination of components and functions has NO ADVERSE IMPACT on the identified design function for the following reasons:

No new malfunctions are created. The Failure Modes and Effects Analysis (FMEA) performed as part of the technical assessment supporting the digital modification concluded that no new types of malfunctions are introduced since the loss of <u>both</u> MFWPs and failures causing an increase in main feedwater flow to the maximum output from both MFWPs are already considered in the licensing basis. Since no new malfunctions are created, the ability to perform the design function "to provide adequate cooling water to the steam generators during normal operation" is maintained.

Using the same initial SSC configuration, proposed activity and UFSAR descriptions 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 UFSAR-Described 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 and control both feedwater pumps.

In this case, the proposed activity is ADVERSE because there is a reduction in the separation of the two original control systems.

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

Example 4-3. Combining Components and Functions with an ADVERSE IMPACT on a UFSAR-Described Design Function

Two non-safety-related analog feedwater control systems and a separate analog control system that controls the main turbine steam-inlet valves 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.

The pertinent UFSAR SSC descriptions are as follows:

(1) Two analog feedwater control systems are identified. The feedwater control system contains a design function "to provide adequate cooling water to the steam generators during normal operation."

(2) One analog main turbine steam-inlet valve control system is identified. The main turbine steam-inlet valve control system contains a design function "to control the amount of steam entering the main turbine during normal operation."

(3) The two feedwater control systems are independent from the main turbine

steam-inlet valve control system.

(4) The function of controlling feedwater is separate from the function of controlling the main turbine steam-inlet valves. This separation is confirmed by a review of the accident analyses that do not include consideration of a simultaneous failure of the feedwater control system and the failure of the turbine control system.

In this case, the proposed activity is ADVERSE because there is a reduction in the separation and independence of the original control systems.

For some component upgrades the likelihood of failure due to software may be judged to be no greater than failure due to other causes, i.e., comparable to hardware common cause failure, and includes no coupling mechanisms. In such a case, even when it affects redundant systems, the digital upgrade would screen out. Considerations for screening relatively simple digital equipment are illustrated in Example 4-A and include:

Commented [PM39]: Placeholder for original NRC comment A39

- The digital modification has a sufficiently low likelihood of common cause failure based on the "qualitative assessment" of system design features, the quality of the design processes employed, and the operating history of the software and hardware used. This qualitative assessment evaluates the magnitude of the adverse effect (i.e., "sufficiently low" likelihood) and which is the focus of the 10 CFR 50.59 evaluation, not the screening. To screen out the digital modification, the following additional considerations provide a greater degree of assurance to conclude that change does not have an adverse effect on a design function:

Formatted: Indent: Left: 1", Bulleted + Level: 1 + Aligned at: 0.5" + Indent at: 1"

- the change is of 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 multiple 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 operating history.

Example 4-A. Screening for a Smart Transmitter (Screens Out)

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 limit scope in that for each channel, the existing 4-20 mA instrument loop is maintained 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. The digital transmitters use a relatively simple digital architecture internally in that the firmware in the new transmitters implements a simple process of acquiring one input signal, setting one output, and performing some simple diagnostic checks. This process runs in a continuous sequence with no branching or interrupts. An alarm relay is available to annunciate detected failures.

Single failures of the digital device are bounded by existing failures of the analog device in that no new digital communications among devices that introduce possible new failure modes involving multiple devices. A "qualitative assessment" of the digital device concluded and the likelihood of common cause failures in multiple channels was very low based on system design features, 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 easily tested. Further, substantial operating history has demonstrated high reliability in applications similar to the ESFAS application.

Consequently, it is concluded that no adverse effects are created, and the change screens out.

Commented [PM40]: Placeholder for original NRC comment A40

Note that an upgrade that is similar to Example 4-A, 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).~~

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

~~Smart transmitters similar to those described in Example 4-1 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. As a result, this change screens in.~~

Commented [PM41]: Placeholder for original NRC comment A41.

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 the reliability of a function whose failure could initiate an accident would be considered to adversely affect a design function...*"

Based on the technical outcomes from applicable Industry and/or NRC guidance documents and using the information considered in those sources to develop those outcomes, the Screen should assess the dependability of performing applicable design functions due to the introduction of software and/or hardware.

Example 4-4 illustrates the application of the dependability consideration.

Example 4-4. Digital Modification that Satisfies Dependability, causing NO ADVERSE IMPACT on a UFSAR-described Design Function

An analog recorder is to be replaced with a new microprocessor-based recorder. The recorder is used for various purposes including Post Accident Monitoring, which is a UFSAR-described design function.

Dependability Assessment: An engineering evaluation performed as part of the technical assessment supporting the digital modification concluded that the new recorder will be highly dependable (based on a quality development process, testability, and successful operating history) and therefore, the risk of failure of the recorder due to software is considered very low.

The change will have NO ADVERSE IMPACT on any design function due to the dependability assessment.

4.2.1.2 Screening of Changes to Procedures as Described in the UFSAR

Commented [A42]: Comments on HSI Screening Guidance were previously provided in:
(1) ML17068A092 Comment Nos. 18-26
(2) ML17170A089 Comment Nos. A17-A27

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, UFSARs will describe any design functions associated with the HSI.

Because the human-system interface (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 3 basic 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.

Formatted: Font: Century Schoolbook, 12 pt

Operators 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 primary types of tasks (Reference: XXX):

(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).

Formatted: Font: Century Schoolbook, 12 pt

To determine potential adverse impacts of HSI modifications on design functions, a two-step analysis must be performed. Step one is assessing how the modification impacts (i.e., *positively*, *negatively* or *no impact*) the operators' abilities to perform each of the four primary types of tasks described above. If there are negative impacts, step two of the analysis consists of determining how the impacts affects the pertinent UFSAR-described design function(s) (i.e., *adversely* or *not adversely*). Examples of negative impacts on operator performance of tasks that may result in adverse effects on a design function include:

- 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.

Formatted: Font: Century Schoolbook, 12 pt

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

[INSERT TABLE 1 FROM HSI COMMENTS FILE HERE.]

~~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.*"

- Because the Human-System Interface involves system/component operation, operator actions, response times, etc., this portion of a digital modification is assessed in this Screen consideration.

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.

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 [e.g., equipment manipulations, actions taken, options available, decision-making, manipulation sequences or operator response times (including the impact of errors of a cognitive nature in which the information being provided is unclear or incorrect)], not the written procedure modifications that may accompany a physical design modification (which are addressed in the guidance provided in NEI 96-07, Section 4.2.1.2).

PHYSICAL INTERFACE WITH THE HUMAN-SYSTEM INTERFACE

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

(a) Physical Interaction with the Human-System Interface (HSI)

(b) Number/Type of Parameters

(c) Information Presentation

(d) Operator Response Time

Physical Interaction with the Human-System Interface

A typical physical interaction modification might involve the use of a touch screen in place of push-buttons, switches or knobs, including sensory-based aspects such as auditory or tactile feedback.

~~To determine if the HSI aspects of a digital modification have an adverse impact on UFSAR-described design functions, potential impacts due to the physical interaction with the HSI should be addressed in the Screen.~~

~~Consideration of a digital modification's impact due to the physical interaction with the HSI involves an examination of the actual physical interface and how it could impact the performance and/or satisfaction of UFSAR-described design functions. For example, if a new malfunction is created as a result of the physical interaction, then the HSI portion of the digital modification would be adverse. Such a new malfunction may be created by the interface requiring the human user to choose which of multiple components is to be controlled, creating the possibility of selecting the wrong component (which could not occur with an analog system that did not need the human user to "make a selection").~~

~~Characteristics of HSI changes that could lead to potential adverse effects may include, but are not limited to:~~

- ~~Changes from manual to automatic initiation (or vice versa) of functions,~~
- ~~Changes in the data acquisition process (such as replacing an edgewise analog meter with a numeric display or a multipurpose CRT in which access to the data requires operator interaction to display),~~
- ~~Changes that create new potential failure modes in the interaction of operators with the system (e.g., new interrelationships or interdependencies of operator actions and/or plant response, or new ways the operator assimilates plant status information),~~
- ~~Increased possibility of mis-operation related to performing a design function,~~
- ~~Increased difficulty for an operator to perform a design function, or~~
- ~~Increased complexity or duration in diagnosing or responding to an accident [e.g., Time-Critical Operation Actions (TCOAs) identified in the UFSAR].~~

~~If the HSI changes do not exhibit characteristics such as those listed above, then it may be reasonable to conclude that the "method of performing or controlling" a design function is not adversely affected.~~

Example~~s~~ 4-5 ~~through 4-7 illustrate the application of the *Physical Interaction* aspect~~ illustrates how to apply the assessment process to ONLY the "controls" element of an HSI.

Example 4-5.* ~~*Physical Interaction*~~ *Assessment of the "Controls" Element of

an HSI with NO ADVERSE IMPACT on a UFSAR-Described Design Function

Description of the Proposed Activity Involving the Control Element:

Currently, a knob is rotated clock-wise to increase a control function and counter clock-wise to decrease the control function. This knob will be replaced with a touch screen. Using the touch screen, touching the "up" arrow will increase the control function and touching the "down" arrow will decrease the control function.

Identification and Assessment of Task Type(s) 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) - NOT INVOLVED

Formatted: Space Before: 0 pt, After: 0 pt, Hyphenate, Tab stops: Not at -0.5"

Design Function Identification:

The UFSAR-described design function states the operator can "increase and decrease the control functions 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 control function).

Identification and Assessment of Modification Impacts on the Task Type(s) INVOLVED:

Formatted: Space Before: 0 pt, After: 0 pt, Hyphenate, Tab stops: Not at -0.5"

As part of the technical evaluation supporting the proposed activity, a Human Factors Evaluation (HFE) was performed. The HFE concluded that no new failures or malfunctions have been introduced as a result of the replacement from a knob to a touch screen.

- possibility of mis-operation - NO IMPACT
- difficulty in evaluating conditions - N/A
- difficulty in performing an action - NO IMPACT
- time to respond - N/A
- new potential failure modes - NO IMPACT

Assessment of Design Function Impact(s)

Using the results from the HFE and examining only the ~~physical interaction aspect~~ "controls" element of an HSI (e.g., ignoring the impact on ~~operator response time or the number and/or sequence of steps necessary to access the new digital controls~~the other three HSI elements), the replacement of the "knob" with a "touch screen" is not adverse since it does not impact the ability of the operator to "increase and decrease the control functions using manual controls located in the Main Control Room," maintaining satisfaction of the UFSAR-described design function.

Using the same proposed activity provided in Example 4-5, Example 4-6 illustrates how a variation in the UFSAR description would cause an adverse impact.

Example 4-6. Physical Interaction with an ADVERSE IMPACT on a UFSAR-Described Design Function

The UFSAR states not only that the operator can "increase and decrease the control functions using manual controls located in the Main Control Room," but also that "the control mechanism provides tactile feedback to the operator as the mechanism is rotated through each setting increment."

Since a touch screen cannot provide (or duplicate) the "tactile feedback" of a mechanical device, replacing the "knob" with a "touch screen" is adverse because it adversely impacts the ability of the operator to obtain tactile feedback from the device.

Using the same proposed activity provided in Example 4-5 and the same UFSAR descriptions from Example 4-6, Example 4-7 illustrates how a variation in the proposed activity would also cause an adverse impact.

Example 4-7. Physical Interaction with an ADVERSE IMPACT on a UFSAR-Described Design Function

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.

Although the operator will now receive auditory "feedback" during the operation of the digital device, the means by which this feedback is provided has been altered. Since the means of controlling the design function has changed, new malfunctions can be postulated (e.g., high ambient sound levels that prevent the operator from hearing the feedback). Therefore, the modification of the feedback feature (i.e., from tactile to auditory) has an adverse impact on the ability of the design function to be performed.

~~**Number and/or Type of Parameters Displayed By and/or Available From the Human-System Interface**~~

~~One advantage of a digital system is the amount of information that can be monitored, stored and presented to the user. However, the possibility exists that the amount of such information may lead to an *over-abundance* that is not necessarily beneficial in all cases.~~

~~To determine if the HSI aspects of a digital modification have an adverse effect on UFSAR-described design functions, potential impacts due to the number and/or type of parameters displayed by and/or available from the HSI should be addressed in the Screen.~~

~~Consideration of a digital modification's impact due to the number and/or type of parameters displayed by and/or available from the HSI involves an examination of the actual number and/or type of parameters displayed by and/or available from the HSI and how they could impact the performance and/or satisfaction of UFSAR-described design functions. Potential causes for an adverse impact on a UFSAR-described design function could include a reduction in the number of parameters monitored (which could make the diagnosis of a problem or determination of the proper action more challenging or time-consuming for the operator), the absence of a previously available parameter (i.e., a type of parameter), a difference in how the loss or failure of parameters occurs (e.g., as the result of combining parameters), or an increase in the amount of information that is provided such that the amount of available information has a detrimental impact on the operator's ability to discern a particular plant condition or to perform a specific task.~~

~~Example 4-8 illustrates the application of the *Number and/or Type of Parameters* aspect.~~

Example 4-8. Number and Type of Parameters with NO ADVERSE IMPACT on a UFSAR-Described Design Function

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). All of these features are described in the UFSAR.

The UFSAR also states that the operator will "examine pump performance and utilize the information from at least one of the redundant plant channels to verify performance" and "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)."

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 does not contain features to automatically control the pump, but does contain the ability to monitor each of the performance indications and inform/alert the operator of the need to take action. Therefore, all pump manipulations will still be manually controlled.

Since the new digital system presents the same number (one) and type (motor electrical current) of pump parameters to directly ascertain pump performance and the same number (three) and type (discharge pressure, flow rate and redundant temperature) of system parameters to indirectly ascertain pump performance, there is no adverse impact on the UFSAR-described design function to perform *direct* monitoring of pump performance and no adverse impact on the UFSAR-described design function to perform *indirect* monitoring of pump performance.

~~Information Presentation on the Human-System Interface~~

~~A typical change in data presentation might result from the replacement of an edgewise analog meter with a numeric display or a multipurpose CRT.~~

~~To determine if the HSI aspects of a digital modification have an adverse effect on UFSAR-described design functions, potential impacts due to how the information is presented should be addressed in the Screen.~~

~~Consideration of a digital modification's impact due to how the information is presented involves an examination of how the actual information~~

~~presentation method could impact the performance and/or satisfaction of UFSAR-described design functions. To determine possible impacts, the UFSAR should be reviewed to identify descriptions regarding how information is presented, organized (e.g., how the information is physically presented) or accessed, and if that presentation, organization or access relates to the performance and/or satisfaction of a UFSAR-described design function.~~

~~Examples of activities that have the potential to cause an adverse effect include the following activities:~~

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

~~If the HSI changes do not exhibit characteristics such as those listed above, then it may be reasonable to conclude that the "method of performing or controlling" a design function is not adversely affected.~~

~~Example 4-9 illustrates the application of the *Information Presentation* aspect.~~

Example 4-9. Information Presentation with an ADVERSE IMPACT on a UFSAR-Described Design Function

A digital modification consolidates system information onto two flat panel displays (one for each redundant channel/train). Also, due to the increased precision of the digital equipment, the increment of presentation on the HSI will be improved from 10 gpm to 1 gpm. Furthermore, the HSI will now present the information layout "by channel/train."

The UFSAR identifies the existing presentation method as consisting of "indicators with a 10 gpm increment" to satisfy safety analysis assumptions and the physical layout as being "by flow path" to allow the operator to determine system performance.

The increase in the display increment is not adverse since the operator will continue to be able to distinguish the minimum increment of 10 gpm UFSAR-described design function.

The new display method (i.e., "by channel/train") adversely affects the ability of the operator to satisfy the design function to ascertain system performance "by flow path."

~~Operator Response Time~~

~~Typically, an increase in the operator response time might result from the need for the operator to perform additional actions (e.g., due to the additional steps necessary to call up or retrieve the appropriate display and operate the "soft" control rather than merely reading an indicator on the Main Control Board).~~

~~To determine if the HSI aspects of a digital modification have an adverse effect on UFSAR-described design functions, potential impacts on the operator response time should be addressed in the Screen.~~

~~Consideration of a digital modification's impact on the operator response time due to the modification of the number and/or type of decisions made, and/or the modification of the number and/or type of actions taken, involves an examination of the actual decisions made/actions taken and how they could impact the performance and/or satisfaction of UFSAR-described design functions. To determine possible impacts, the UFSAR must be reviewed to identify descriptions relating to operator response time requirements and if those timing requirements are related to the performance and/or satisfaction of a UFSAR-described design function.~~

~~Example 4-10 is the same as Example 4-9, but illustrates the application of the *Operator Response Time* aspect.~~

Example 4-10. Operator Response Time with NO ADVERSE IMPACT on a UFSAR-Described Design Function

A digital modification consolidates system information onto two flat panel displays (one for each redundant channel/train). Also, due to the increased precision of the digital equipment, the increment of presentation on the HSI will be improved from 10 gpm to 1 gpm. Furthermore, the HSI will now present the information layout "by channel/train."

The UFSAR identifies the existing presentation method as consisting of the physical layout as being "by flow path" to allow the operator to determine system performance.

Although the UFSAR identifies the existing presentation method as consisting of a physical layout "by flow path" to allow the operator to determine system performance and the new display method (i.e., "by channel/train") will require additional steps by the operator to determine system performance, requiring more time, there is no adverse impact on satisfaction of the design function to ascertain system performance because no response time requirements are applicable to the design function of the operator being able "to determine system performance."

COMPREHENSIVE HUMAN-SYSTEM INTERFACE EXAMPLE

Although no additional guidance is provided in this section, Example 4-11 illustrates how each of the aspects identified above would be addressed.

Example 4-11. Digital Modification involving Extensive HSI Considerations with NO ADVERSE IMPACTS on a UFSAR-Described Design Function

Component controls for a redundant safety-related system are to be replaced with PLCs. The existing HSI for these components is made up of redundant hard-wired switches, indicator lights, and analog meters. The new system consolidates the information and controls onto two flat panel displays (one per redundant train), each with a touch screen providing “soft” control capability.

The existing number and type of parameters remains the same, which can be displayed in a manner similar to the existing presentations (e.g., by train). However, the information can be also presented in different configurations that did not previously exist (e.g., by path or by parameter type to allow for easier comparison of like parameters), using several selectable displays.

The flat panel display can also present any of several selectable pages depending on the activity being performed by the operator (e.g., starting/initiating the system, monitoring the system during operation, or changing the system line-up).

To operate a control, the operator must (via the touch screen) select the appropriate activity (e.g., starting/initiating the system, monitoring the system during operation, or changing the system line-up), select the desired page (e.g., train presentation, path presentation, or parameter comparison), select the component to be controlled (e.g., pump or valve), select the control action (e.g., start/stop or open/close), and execute it.

The display remains on the last page selected, but each page contains a "menu" of each possible option to allow direct access to any page without having to return to the "main menu."

The two new HSIs (one per redundant train) will provide better support of operator tasks and reduced risk of errors due to:

- Consolidation of needed information onto a single display (within the family of available displays) that provides a much more effective view of system operation when it is called into action.

- Elimination of the need for the operator to seek out meter readings or indications, saving time and minimizing errors.
- Integration of cautions and warnings within the displays to help detect and prevent potential errors in operation (e.g., warnings about incorrect system lineups during a test or maintenance activity).

The design was developed using a human factors engineering design, with a verification and validation process consistent with current industry and regulatory standards and guidelines. As part of the technical evaluation supporting the proposed activity, a Human Factors Evaluation (HFE) was performed. Based on the conclusions from the HFE, the design provides a more effective HSI that is less prone to human error than the existing design.

The UFSAR-described design functions applicable to this proposed activity include ~~descriptions of~~ how the existing controls, including the physical switches, indicator lights and meters, ~~and how~~ each of these SSCs is used during normal and abnormal (including accident) operating conditions. The ~~UFSAR identifies the~~ current physical arrangement (i.e., two physically separate locations) ~~as providing a~~ provides assurance that the design function is satisfied by preventing the operator ~~that prevents the operator~~ from operating the "wrong" component. There are no UFSAR-described design functions related to the operator response times associated with using the existing controls.

The impacts on design functions are identified below:

- *Physical Interaction* - NOT ADVERSE because the new HSI consists of two physically separate displays.
- *Number and Type of Parameters* - NOT ADVERSE because the same number and type of parameters exist with the new HSI.
- *Information Presentation* - NOT ADVERSE because all of the existing features (e.g., individual controls, indicator lights and parameters displays that mimic the analog meters) continue to exist with the new HSI.
- *Operator Response Time* - NOT ADVERSE because no response time requirements were applicable to any of the design functions and there were no indirect adverse affects on any other design function.

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

In the following sections and sub-sections that describe the Evaluation guidance ~~unique to~~particularly useful~~l~~ 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.

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

~~Credibility of~~ Common Cause Failure (CCF) Likelihood Determination Outcomes

The possible outcomes of an engineering evaluation (e.g., CCF Susceptibility Analysis), performed in accordance with ~~regarding a CCF from the CCF Susceptibility Analysis performed in accordance with applicable~~ Industry and/or NRC ~~approved~~ guidance documents, regarding the CCF likelihood are as follows:

(1) CCF likelihood ~~not credible (i.e., likelihood of a CCF caused by an I&C failure source is NOT greater than the likelihood of acomprable to CCF caused by other failure sources that are not considered specifically analyzed in the UFSAR)~~sufficiently low (as defined in Definition 3.17)

(2) CCF likelihood ~~credible (i.e., likelihood of a CCF caused by an I&C failure source IS greater than or equalcomprable to the likelihood of a CCF caused by other failure sources that are considered specifically analyzed in the UFSAR)~~not sufficiently low

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

~~Failure Analysis~~

~~As described in SECY 91-292 regarding NRC review of advanced light water reactor (ALWR) designs, digital I&C systems employ a greater degree of sharing of data transmission, functions, and process equipment as compared to analog systems. While this sharing enables some of the key benefits of digital equipment, it also increases the potential consequences of individual failures.~~

~~Consideration of potential system failures and undesirable behaviors should be an integral pairt of the process of designing, specifying, and implementing a digital upgrade. Consideration of these undesirable events is referred to collectively as failure analysis. Failure analysis interacts with essentially all~~

Commented [A43]: Source: ML13298A787 Concern 3
Comment: The overarching goal is to have clear guidance. That is, both licensees and inspectors must interpret this document the same way.

The reason that NEI 01-01 was written was because it was felt that it was not clear how to apply NEI 96-07 to digital modifications, because digital based SSCs were typicaly different that analog systems in certian ways.

The typical ways in which new digital electronics SSCs are different are:
(1) Modes Behaviour & Misbehaviour
(2) Combining of Functions
(3) Coupling of Functions
(4) Potential for Increased Complexity
(5) System Architecture Changes
(6) Contain Software
While some of these aspects are considered in the screening section, the evaluation is silent on those that are addressed in the screening section.

The failure analysis section below was added to address this comment.

Formatted: Highlight

Commented [A44]: Source: Engineering Judgement
Rationale: There are two things of concern:
(1) Determination of if CCF is credible
(2) Characterisation of behavior during CCF ... [1]

Commented [A45]: Source:
(1) ML17068A092 Comment No. 12
(2) ML17170A089 Comment No. A4
Rationale: New terms should be defined since undefined terms are a source of regulatory uncertainty.

Commented [A46]: In the August 29 Public Meeting, NEI stated the terms "CCF Credible/Not Credible" will no longer be used. All instances of "credible" have been highlighted to facilitate making this change.

Formatted: Highlight

Commented [A47]: Source: ML17170A089 Comment No. A30
Rationale: There are many ways that CCF can be considered in the FSAR (as updated), specifically postulating and analyzing the results being only one.

Formatted: Highlight

Commented [A48]: Source: ML17170A089 Comment No. A30
Rationale: There are many ways that CCF can be considered in the FSAR (as updated), specifically postulating and analyzing the results being one one.

Commented [A49]: Source: The following text (except as noted) adapted from NEI 01-01 Section 5.1 & 5.1.1.
Rationale: To address the first comment in Section 4.3 above.

Commented [A50]: Source: Source: ML13298A787 - Concern 11
Rationale: Text adapted from NEI 01-01 Section Section 5.3.1 to address the first comment in Section 4.3 above.

the main elements of the design process. It provides information needed to support the licensing evaluations, and it provides the context in which the digital upgrade issues ultimately can be resolved. Failure analysis examines what you do not want the system or device to do.

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

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

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

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

- Assessment of the significance and risk of identified vulnerabilities.

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

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

Ultimately, the digital equipment is installed to support overall system requirements, which in turn are necessary to support the plant system-level requirements. It is generally at the plant system level that major functional requirements exist to support plant safety and availability. Consequently,

~~failure analysis should start by identifying the system or "design function" level functions, and examining how the digital equipment can cause these functions not to be performed.~~

~~In addition to failures of the system to perform its function, other failures such as spurious actions, challenges to safety systems, transient or accident initiators, etc., should be examined.~~

Engineering Evaluation Topics Beneficial for Performing a 50.59 Evaluation of Digital-Specific Adverse Effects

~~For digital modifications, attention should be given to the major things that may be different in the new digital electronic equipment, for example:~~

In the preparation of responses to the Evaluation criteria, the outcomes from the following engineering evaluation topics should be considered (as necessary):

(1) Modes of Behaviour and Misbehaviour
(2) Combining of Functions
(3) Coupling of Functions (e.g., via digital communications)
(4) Potential for Increased Complexity
(5) System Architecture Changes
(6) Software

Items 1, 2, 3, & 5 have the most potential to create the possibility for accidents of a different type and/or malfunctions with a different result.

~~Items 4 & 6 can make it more difficult to fully understand all aspects of the modification.~~

Commented [A51]: **Source:** ML13298A787
Modes of Beaviour and Misbehaviour - Concern 11
Combining of Functions - Concerns 5 & 7
Coupling of Functions - Concern 10
Complexity - Concern 1
Rationale: To address the first comment in Section 4.3 above, one must identify the important aspects to consider.

Examples

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 ~~few~~ non-safety-related systems that, upon failure, can initiate an accident. Furthermore, a failure of the MFW system is one of the ~~few~~ malfunctions that are also accident initiators.

Commented [A52]: **Source:** ML170170A089 Comment No. A6.
Rationale: Based on the definition of "accident" in NEI 96-07, many accidents are initiated by non-safety related SSCs. (Note: safety related SSCs are tpicaly credited to miigate accidents.)

Commented [A53]: **Source:** ML170170A089 Comment No. A6.
Rationale: Based on the definition of "accident" in NEI 96-07, many accidents are initiated by non-safety related SSCs. (Note: safety related SSCs are tpicaly credited to miigate accidents.)

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:

> "*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 includes items unique to digital and items not unique to digital. An example of an item unique to digital is consideration of the impact on accident frequency due to a software CCF, which will be addressed in the guidance in this section. An example of a~~n item~~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 for applicable regulatory requirements~~,~~ and ~~commitments~~ other acceptance criteria to which the licensee is committed, and departures from standards as outlined in the general design criteria, as ~~described~~ 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 ~~causal relationship (i.e.,~~ *attributable* (i.e., causal relationship~~or not~~) and the ~~magnitude of the effect~~

Commented [A54]: Source: ML17170A089 Comment No. A34
Rationale: Please change "CCF" to "software CCF" as appropriate. CCF has always been, and continues to be, a regulatory concern, and it is addressed in many ways in the SARs (as is explained in Section 2 above).

Commented [A55]: Source: ML17170A089 Comment No. A34
Rationale: CCF has always been, and continues to be, a regulatory concern, and it is addressed in many ways in the SARs (as is explained in Section 2 above).

Commented [A56]: Source: ML17170A089 Comment No. A35
Rationale: By adding this text, the reference was change forom a general section reference, to a reference to the specific applicable paragraph and example (to be explicitly clear what part of 4.3.1 was being reffered to). The point is: Not meeting applicalbe technical criteria should be considered as "not compatible with 'not more then a minimal increase' " standard.

Commented [A57]: Source: ML17170A089 Comment No. A40
Rationale: Clarification: The term attributable, since it is not defined, is used in the common English sence (i.e., indicationg causality).

~~(i.e.,~~ *negligible/discernable* (i.e., magnitude) criteria from NEI 96-07, Section 4.3.1 will be examined in the guidance in this section.

GUIDANCE

Factors to Consider and Address in the Response

1. Use of Software

Software developed in accordance with a defined life cycle process, and 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 change process and the design documentation contain the information that will be used to determine if software increases the frequency 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 ~~change~~ process and the design documentation contain the information that will be used to determine if the use of digital components increases the frequency of an accident.

3. Creation of a Software Common Cause Failure (Software CCF)

An engineering evaluation of the ~~quality~~ design and design processes determine~~s~~ the likelihood of failure due to software via a common cause failure and its potential impact on the frequency of an accident. The engineering evaluation that assesses CCF likelihood includes the possible outcomes (i.e., CCF likelihood is sufficiently low or CCF likelihood is not sufficiently low). ~~This information is documented in the qualitative assessment of the potential contributors to CCF and disposition of whether~~

Commented [PM58]: Placeholder for original NRC comment A58

Commented [A59]: **Source:** ML17170A089 Comment No. A37
Rationale: Sotware development proceses and software design are two distinct things, and each should be addressed separately.

Commented [A60]: **Source:**
(1) ML13298A787 - Concern 9
(2) ML17170A089 Comment No. A37 & A39
Rationale: Sotware development proceses and software design are two distinct things, and each should be addressed separately.

Commented [A61]: Check to assure useage matches definition.

~~the design effectively reduced the likelihood of the CCF to the extent that the CCF can be considered not credible (e.g., in a CCF Susceptibility Analysis).~~

4. 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 an accident.

5. 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., external watchdog timers, isolation devices, segmentation, self-testing and self-diagnostic features)
- Non-concurrent Triggers
- Sufficiently Simple (i.e., enabling comprehensive 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)

Determination of ~~Causality (using~~ Attributable (i.e., causality)

If a CCF is determined to be not credible, then there is NO ~~*attributable*~~ *dicernable* impact on the frequency of occurrence of an accident. Namely, if a CCF is sufficiently unlikely to occur, then no mechanism for an ~~attributable~~ discernable impact has been created.

If a CCF is determined to be credible, but the component/system is not an accident initiator, then there is NO *attributable* impact on the frequency of

Formatted: Highlight

Commented [A62]: Should expand based on recent draft RIS after RIS language has been finalized.

Commented [A63]: **Source:** ML17170A089 Comment No. A40
Rationale: This section uses the term “atributble” in the same way that it iuses Negligible/Dicernable; to indicate magnitude of effect. The wording was changed to more clearly indicate causality rather than magnitude of effect as is the convention in the standard English interpretation of “attributable”.

Formatted: Highlight

Commented [A64]: **Source:** ML17170A089 Comment No. A40
Rationale: The word “attributable” is about causality and the word “discernable” is related to magnitude of effect. The term “not credible” means a suficently low probability (so that it need not be considered), not that it is imposible. Only if CCF is impossible can there be no attributable impact.

This paragraph should be moved after the next one, or moved to the next section.

Formatted: Highlight

occurrence of an accident. Namely, even if a CCF does occur, there is no relationship between the CCF and the accident initiator(s).

Commented [A65]: **Source:** ML17170A089 Comment No. A40
Rationale: This section uses the term “atributble” in the same way that it iuses Negligible/Dicernable; to indicate magnitude of effect. The wording was changed to more clearly indicate causality rather than magnitude of effect as is the convention in the standard English interpretation of “attributable”.

Example 4-12 illustrates the case of NO *attributable* impact on the frequency of occurrence of an accident for a SSC not being an accident initiator.

Example 4-12. NO ATTRIBUTABLE Impact on the Frequency of Occurrence of an Accident Due to a SSC Not Being an Accident Initiator

<u>Proposed Activity</u>

Two safety-related containment chillers exist. There are two analog control systems (one per chiller) that are physically and functionally the same.

Each analog control system will be replaced with a separate digital control system. The hardware platform for each digital control system is from the same supplier and the software in each digital control system is exactly the same.

<u>Affected Accidents and Accident Initiators</u>

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 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 in both cases 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.

<u>Impact on Accident Frequency</u>

In this case, the safety-related containment chillers are not related to the accident initiators (i.e., pipe breaks). Furthermore, the chillers are only considered as part of accident mitigation; <u>after</u> 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.

If a ~~CCF is determined to be credible~~ ~~and the~~ component/system is an accident initiator, then there is an *attributable* potential impact on the frequency of occurrence of the accident.

Example 4-13 illustrates the case of an *attributable* potential impact on the frequency of occurrence of an accident for the SSC being an accident initiator.

Example 4-13. ATTRIBUTABLE Potential Impact on the Frequency of Occurrence of an Accident Due to a SSC Being an Accident Initiator

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.

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

Based on the technical outcome from ~~the CCF Susceptibility Analysis and~~ the Failure Modes and Effects Analysis (FMEA) performed as part of the technical assessment supporting this digital modification, a software CCF causing the loss of both feedwater control systems (resulting in the loss of both MWFPs and/or the closure of both MFWP flow control valves) has been determined to be attributable ~~credible.~~ (i.e., Since the failure of the digital feedwater control systems can cause the loss of MFWPs or the closure of MFWP flow control valves, a potential impact on accident frequency due to the CCF can be *attributed* to the digital modification.

Determination of Magnitude (using *Negligible/Discernable*)

Commented [A66]: **Source:** ML17170A089 Comment No. A40
Rationale: The word "attributable" is about causality and the word "discernable" is related to magnitude of effect. The term "not credible" means a suficently low probability (so that it need not be considered), not that it is imposible. Only if CCF is impossible can there be no attributable impact.

Commented [A67]: **Source:** ML17170A089 Comment No. A40
Rationale: The word "attributable" is about causality and the word "discernable" is related to magnitude of effect. The term "not credible" means a suficently low probability (so that it need not be considered), not that it is imposible. Only if CCF is impossible can there be no attributable impact.

Commented [A68]: **Source:** ML17170A089 Comment No. A40
Rationale: The word "attributable" is about causality and the word "discernable" is related to magnitude of effect. The term "not credible" means a suficently low probability (so that it need not be considered), not that it is imposible. Only if CCF is impossible can there be no attributable impact.

For the case in which ~~a CCF is credible and~~ there is an attributable potential impact on the frequency of occurrence of an accident, the magnitude portion of the criteria (i.e., *negligible/discernable*) also needs to be assessed.

Commented [A69]: Source: ML17170A089 Comment No. A40
Rationale: The word "attributable" is about causality and the word "discernable" is related to magnitude of effect. The term "not credible" means a suficently low probability (so that it need not be considered), not that it is imposible. Only if CCF is impossible can there be no attributable impact.

To determine the overall effect of the digital modification on the frequency of an accident, examination of all the factors associated with the digital modification and their interdependent relationship need to be considered.

To achieve a *negligible* conclusion, the examination of all the factors would conclude that the net 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)***" [***emphasis*** added] due to the net effect of the factors considered (i.e., use of software, use of digital components, creation of a software CCF , intended benefits and design attributes/features).

Alternately, if the net effects are such that a clear trend towards increasing the frequency would result, a *discernable* increase in the accident frequency would exist. However, to remain consistent with the guidance provided in NEI 96-07, Section 4.3.1, a *discernable* increase in the accident frequency may~~would~~ 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~~were not~~ met.

Commented [A70]: Source: ML17170A089 Comment No. A45 & A46
Rationale: Standards are generally design neutral. That is problems could occur due to (1) not meeting standards, and (2) poor design. Standards are only one of the criteria that can cause increases, so meeting all design standards may not be enough; however, failing to meet standards may be ok, but must be reviewed by the NRC staff.

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

Example 4-14 illustrates the NEGLIGIBLE impact case.

Example 4-14. NEGLIGIBLE Impact on the Frequency of Occurrence of an Accident

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.

Attributable Conclusion

See Example 4-13.

Magnitude Conclusion

Factors Considered:

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. CCF - Not Credible

Formatted: Highlight

4. Benefits - Reliability and performance increased

5. Design Attributes/Features - [LATER]

The net change in the frequency of occurrence of the Loss of Feedwater event is ***negligible*** due to the net effect of the factors considered.

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.

987 Example 4-15 illustrates the DISCERNABLE increase case.

Example 4-15. DISCERNABLE Increase in the Frequency of Occurrence of an Accident

Proposed Activity

Same as Example 4-14.

Attributable Conclusion

See Example 4-13.

Magnitude Conclusion

Factors Considered:

1. Software - Same as Example 4-14.

2. Digital Components - Same as Example 4-14.

3. CCF - Credible

4. Benefits - Same as Example 4-14.

5. Design Attributes/Features - Same as Example 4-14

Requirements/Standards Consideration

All applicable NRC requirements, as well as design, material and construction standards, continue to be met.

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

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 CCF being credible. However, even with a clear trend towards increasing the frequency, the satisfaction of all applicable NRC requirements, as well as design, material and construction standards, means that there is NOT more than a minimal increase in the frequency of occurrence of the accident due to the digital modification.

988

Formatted: Highlight

Formatted: Highlight

HUMAN-SYSTEM INTERFACE ASSESSMENT

If no personnel-based initiators (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 and the magnitude criterion (i.e., *negligible/discernable*) are assessed utilizing the guidance described in NEI 96-07, Section 4.3.1.

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 software CCF, which will be addressed in the guidance in this section. An example of an item 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 guidance described in NEI 96-07, Section 4.3.2.

Commented [A71]: Make same changes as in 6th paragraph of the introduction of Section 4.3.1.

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* and the magnitude (i.e., *negligible/discernable*) criteria from NEI 96-07, Section 4.3.2 will be examined in the guidance in this section.

GUIDANCE

Factors to Consider and Address in the Response

1. Use of Software

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

Commented [A72]: Reword in similar manner as in Section 4.3.1, after agreement is reached there.

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 (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 change process and the design documentation contain the information that will be used to determine if the use of digital components increases the likelihood of a malfunction.

Commented [A73]: Reword in similar manner as in Section 4.3.1, after agreement is reached there.

3. Creation of a Software Common Cause Failure

An engineering evaluation of the quality and design processes determines the likelihood of failure due to software via a common cause failure and its potential impact on the likelihood of a malfunction. This information is documented in the qualitative assessment of the potential contributors to CCF and disposition of whether the design effectively reduced the likelihood of the CCF to the extent that the CCF can be considered not credible (e.g., in a CCF Susceptibility Analysis).

Formatted: Highlight

Commented [A74]: Reword in similar manner as in Section 4.3.1, after agreement is reached there.

Commented [A75]: Source NEI 96-07r1. Also revise to reflect the following from the 50.59 Q&A document.: Section 4.3.2 of NEI 96-07, R1, says that a change that reduces system/equipment redundancy, diversity, separation or independence requires prior NRC approval. Does this mean reductions from redundancy, diversity, separation or independence described in the UFSAR? Or is prior NRC approval required only if the change reduces redundancy, diversity, separation or independence below the level required by the regulations?

A. A change that reduces redundancy, diversity, separation or independence of UFSAR-described design functions is considered more than a minimal increase in the likelihood of malfunction and requires prior NRC approval. Licensees may, however, without prior NRC approval, reduce excess redundancy, diversity, separation or independence, if any, to the level credited in the UFSAR.

~~Example 6~~

~~The change would reduce system/equipment redundancy, diversity, separation or independence.~~

A change that reduces redundancy, diversity, separation or independence of UFSAR-described design functions is considered more than a minimal increase in the likelihood of malfunction and requires prior NRC approval. Licensees may, however, without prior NRC approval, reduce excess redundancy, diversity, separation or independence, if any, to the level credited in the UFSAR. "As credited in the safety analysis" is discussed in NEI 96-07, Section 3.3.

4. 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 a malfunction.

5. Design Attributes/Features

Commented [A76]: Reword in similar manner as in Section 4.3.1, after agreement is reached there.

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., external watchdog timers, isolation devices, segmentation, self-testing and self-diagnostic features)
- Non-concurrent Triggers
- Sufficiently Simple (i.e., enabling comprehensive 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 ~~S~~CCF is possible)
- Failure State (e.g., always known to be acceptable)

Determination of Attributable

If a CCF is determined to be not credible, then there is NO *attributable* impact on the likelihood of occurrence of a malfunction. Namely, if a CCF is

Formatted: Highlight

sufficiently unlikely to occur, then no mechanism for an attributable impact has been created.

If a CCF is determined to be credible, but the component/system is not a malfunction initiator, then there is NO *attributable* impact on the likelihood of occurrence of a malfunction. Namely, even if a CCF does occur, there is no relationship between the CCF and the malfunction initiator(s).

Example 4-16 illustrates a case of NO *attributable* impact on the likelihood of occurrence of a malfunction for a SSC not being a malfunction initiator.

Example 4-16. ~~NO~~ ATTRIBUTABLE Impact on the Likelihood of Occurrence of a Malfunction Due to a SSC Not Being a Malfunction Initiator

Proposed Activity

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 one safety-related containment chiller. The UFSAR identifies two equipment-related initiators: (a) failure of the Emergency Diesel Generator (EDG) to start (preventing the EDG from supplying electrical power to the containment chiller it powers), (b) an electrical failure associated with the chiller system (e.g., feeder breaker failure) or a mechanical failure within the chiller itself (e.g., flow blockage).

Impact on Malfunction Likelihood

In this case, the safety-related chiller control system is not related to the malfunction initiators (i.e., EDG failure, breaker failure or chiller failure). ~~Therefore~~However,, there is ~~NO~~ may be an impact on the likelihood of occurrence of the malfunction that can be *attributed* to the digital modification.

If a ~~CCF is determined to be credible and the~~ component/system is a malfunction initiator, then there is an *attributable* potential impact on the likelihood of occurrence of the malfunction.

Formatted: Highlight

Commented [A77]: Reword in similar manner as in Section 4.3.1, after agreement is reached there.

Commented [A78]: **Source:** ML17170A089 Comment No. A40
Rationale: Consistent with use of "attributable" to as indication causality.

Commented [A79]: **Source:** ML17170A089 Comment No. A40
Rationale: Consistent with use of "attributable" to as indication causality.

Commented [A80]: Make similar to words in Section 4.3.1.

Example 4-17 illustrates the case of an *attributable* potential impact on the likelihood of occurrence of a malfunction for the SSC being a malfunction initiator.

Example 4-17. ATTRIBUTABLE Potential Impact on the Likelihood of Occurrence of a Malfunction Due to a SSC Being a Malfunction Initiator

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.

Affected Malfunction and Malfunction Initiator

The affected malfunction is the loss of a MFWP or the closure of a MFWP flow control valve. The UFSAR identifies an equipment-related initiator as involving the failure of a feedwater control system.

Impact on Malfunction Initiator

Based on the technical outcome from the CCF Susceptibility Analysis and the Failure Modes and Effects Analysis (FMEA) performed as part of the technical assessment supporting this digital modification, a software CCF causing the loss of both feedwater control systems (resulting in the loss of both MWFPs and/or the closure of both MFWP flow control valves) has been determined to be credible.

Since the failure of the feedwater control systems can cause the loss of MFWPs or the closure of MFWP flow control valves, a potential impact on malfunction likelihood due to the CCF can be *attributed* to the digital modification.

Determination of Magnitude (using *Negligible/Discernable*)

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

Formatted: Highlight

Commented [A81]: Source: ML17170A089 Comment No. A40
Rationale: Consistent with use of "attributable" to as indication causality.

To determine the overall effect of the digital modification on the likelihood of a malfunction, examination of all the factors associated with the digital modification and their interdependent relationship need to be considered.

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)***"[***emphasis*** added] due to the net effect of the factors considered (i.e., use of software, use of digital components, creation of a software CCF, intended benefits and design attributes/features).

Alternately, if the net effects are such that a clear trend towards increasing the likelihood would result, a *discernable* increase in the malfunction likelihood would exist. However, to remain consistent with the guidance provided in NEI 96-07, Section 4.3.2, a *discernable* increase in the malfunction likelihood would NOT be more than minimal if applicable NRC requirements, as well as design, material, and construction standards, continue to be met.

Commented [A82]: Change to be the same as Section 4.3.1 wording after agreement is reached.

Examples 4-18 and 4-19 will examine the magnitude portion (i.e., *negligible/discernable*) of the criteria and assume the *attributable* portion of the criteria has been satisfied.

1136 Example 4-18 illustrates the NEGLIGIBLE impact case.

Example 4-18. NEGLIGIBLE Impact in the Likelihood of Occurrence of a Malfunction

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.

Attributable Conclusion

See Example 4-17.

Magnitude Conclusion

Factors Considered:

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. CCF - Not Credible

4. Benefits - Reliability and performance increased

5. Design Attributes/Features - [LATER]

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

Formatted: Highlight

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.

1137 Example 4-19 illustrates the DISCERNABLE increase case.

Example 4-19. DISCERNABLE Increase in the Likelihood of Occurrence of a Malfunction

Proposed Activity

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."

Attributable Conclusion

In this case, the safety-related main control room chiller control system is related to a malfunction initiator (i.e., loss of logic and/or operation function) of the safety injection pumps. Therefore, there is a potential impact on the likelihood of occurrence of the malfunction that can be *attributed* to the digital modification.

Magnitude Conclusion

Factors Considered:

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. CCF - Credible

Formatted: Highlight

4. Benefits - Reliability and performance increased

5. Design Attributes/Features - [LATER].

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.

Requirements/Standards Consideration

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 credible, which does not satisfy the NRC requirements associated with systems/components that must satisfy single failure requirements. With a clear trend toward increasing the likelihood and the failure to satisfy an NRC requirement, there is more than a minimal increase in the likelihood of occurrence of the malfunction of both safety injection pumps due to the digital modification.

Formatted: Highlight

HUMAN-SYSTEM INTERFACE ASSESSMENT

If no personnel-based initiators (e.g., operator error) are identified among the accident 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 and the magnitude criterion (i.e., *negligible/discernable*) 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?

<u>INTRODUCTION</u>

From NEI 96-07, Section 3.2:

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

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

From NEI 96-07, Section 4.3.5, the two considerations that need to be assessed when answering this Evaluation question are *credible* and *bounded/related.*

Formatted: Highlight

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 a CCF likelihood is determined to be ~~not credible~~sufficiently low, then the creation of a possibility for an accident of a different type is NOT credible ~~because there is no mechanism for the possibility of an accident of a different type to be created and possible accidents of a different type are limited to those that are as likely to happen as those previously evaluated in the UFSAR~~.~~[2]~~

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

Determination of Bounded/Related

For the case in which ~~a CCF~~ an accident of a different type is credible, the *bounded/related* portion of the criteria also needs to be assessed.

Events/sequences currently considered in the UFSAR form the basis for comparison of events, which makes it possible to identify and evaluate the limiting case.

The UFSAR evaluates a broad spectrum of accidents (i.e., initiating *events* and the *sequences* that result from various combinations of plant and safety systems response). Accidents are categorized according to expected frequency of occurrence and by type. The accident type is defined by its effect on the plant (e.g., decrease in heat removal by the secondary system, increase in heat removal by the secondary system, etc.). Characterization of accidents by type provides a basis for comparison based on *events/sequences*, which makes

~~[2] Refer to NEI 96-07, Section 4.3.5, 3rd paragraph.~~

Formatted: Highlight
Formatted: Highlight
Formatted: Font: Not Italic, Highlight
Formatted: Highlight
Formatted: Font: Not Italic, Highlight
Formatted: Highlight

it possible to identify and evaluate the limiting cases (i.e., the cases that can challenge the analysis acceptance criteria) and eliminate non-limiting cases from further consideration.

Therefore, a new accident that is of the same type (i.e., its effect on the plant is the same)~~,~~ and is within the same expected frequency of occurrence ~~, and results~~ meets the *bounded* criterion. ~~Alternately,~~ For a new accident that is NOT of the same type~~, if~~ (i.e., its effect on the plant is different)~~,~~ and/or is NOT within the same expected frequency of occurrence~~, or result~~ ~~does NOT meet~~ the *bounded* criterion does not apply.

Accidents of a different type are credible accidents that the proposed activity could create that have an impact on the type of *events/sequences* previously evaluated in the UFSAR. Namely, a **different/new** accident analysis would be needed for this different type of accident, ~~not just~~or a **revision** of a current accident analysis.

Therefore, a **different/new** accident analysis would NOT be related to an event already been analyzed. Alternately, the revision of a current accident analysis would be related to an event already analyzed, and a determination is needed if the already analyzed events bounds the new event in both frequency and results.

Example 4-20 illustrates the ~~NO~~ CREATION of the possibility of an accident of a different type case.

Example 4-20. ~~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

Commented [PM83]: Placeholder for original NRC comment A83.

Formatted: Highlight

Commented [A84]: Source: ML17170A089 Comment No. A67 & A69
Rationale: These changes are necessary in order to be consistent with the newest version of RG 1.187.

Commented [A85]: Source: ML17170A089 Comment No. A67 & A69
Rationale: These changes are necessary in order to be consistent with the newest version of RG 1.187.

Commented [A86]: Source: ML17170A089 Comment No. A67 & A69
Rationale: These changes are necessary in order to be consistent with the newest version of RG 1.187.

Commented [A87]: Source: ML17170A089 Comment No. A67 & A69
Rationale: These changes are necessary in order to be consistent with the newest version of RG 1.187.

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 the technical outcome from the CCF Susceptibility Analysis and the Failure Modes and Effects Analysis (FMEA) performed as part of the technical assessment supporting this digital modification, a software CCF causing the loss of both feedwater control systems (resulting in the loss of both MWFPs) has been determined to be credible.

Therefore, in this case, a new accident has been created.

Bounded/Related Conclusion

Although the CCF causes the loss of both feedwater pumps, potentially challenging the analysis acceptance criteria (which is the focus of Evaluation Question #7), the loss of both feedwater pumps still causes the same type of accident (i.e., a decrease in heat removal by the secondary system).

As identified in the UFSAR, the Loss of Feedwater event considered the loss of one main feedwater pump, allowing the safety analysis to credit a certain amount of flow from the remaining operational feedwater pump. Even though the CCF could disable both feedwater pumps, the accident type and category ~~remain~~ may not be *bounded* by a *related* accident because the *new* event would not require a "new" accident analysis, only a revision to the input parameter(s) and/or assumption(s) used in the current Loss of Feedwater accident analysis related to the operational status of the feedwater pumps. Therefore, the proposed activity ~~does not~~may create the possibility of an accident of a different type.

Example 4-21 illustrates the CREATION of the possibility of an accident of a different type case.

Formatted: Highlight

Formatted: Highlight

Commented [A88]: Source: ML17170A089 Comment No. A67 & A69
Rationale: These changes are necessary in order to be consistent with the newest version of RG 1.187.

Example 4-21. 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

Formatted: Highlight

Based on the technical outcome from the CCF Susceptibility Analysis and the Failure Modes and Effects Analysis (FMEA) performed as part of the technical assessment supporting this digital modification, a software CCF impacting both the feedwater control systems and the main turbine steam-inlet valves control system has been determined to be credible.

Formatted: Highlight

Therefore, in this case, the following conditions are credible:

Formatted: Highlight

(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)

Conditions (1) though (4) are already considered in the UFSAR, so these do not create a new accident. Since conditions (1) through (4) do not create a new accident, they do not create the possibility for an accident of a different type.

Conditions (5) through (8) are not considered in the UFSAR, so four new accidents have been created.

Bounded/Related Conclusion

Based on the current set of accidents identified in the UFSAR, the UFSAR accident 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.

The new accidents created in Conditions (5) though (8) are NOT *bounded* by a *related* accident because new accident analyses will be needed. Therefore, the proposed activity does create the possibility of an accident of a different type.

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

INTRODUCTION

From NEI 96-07, Section 4.3.6, the two considerations that need to be assessed when answering this question are ~~*credible*~~ as likely to happen as those described in the UFSAR and *bounded*.

Formatted: Highlight

GUIDANCE

Determination of ~~Credible~~ as likely to happen as those described in the UFSAR

Formatted: Highlight

From NEI 96-07, Section 4.3.6:

> "*The possible malfunctions with a different result are limited to those that are as likely to happen as those described in the UFSAR.*"

If a CCF likelihood is determined to be ~~not credible~~ sufficiently low, then the ~~creation of a~~ possibility for a malfunction with a different result is NOT ~~*credible*~~as likely to happen as those described in the UFSAR ~~because there is no mechanism for the possibility of a malfunction with a different result to be created and possible malfunctions with a different result are limited to those that are as likely to happen as those previously evaluated in the UFSAR~~.~~[3]~~

If a CCF likelihood is determined to be ~~credible~~not sufficiently low, then the ~~creation of a~~ possibility for a malfunction with a different result is ~~*credible*~~ as likely to happen as those described in the UFSAR.

Determination of Bounded

For the case in which a ~~CCF~~ possibility for a malfunction with a different result is ~~credible~~ as likely to happen as those described in the UFSAR, the *bounded* portion of the criteria also needs to be assessed.

Types of Malfunctions to be Considered:

NEI 96-07, Section 4.3.6 states:

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

Based on this excerpt, both previously-evaluated malfunctions and new malfunctions need to be considered when developing the response to this Evaluation question. Typically, a new FMEA will be necessary for a digital modification since the original considerations for malfunctions did not take into account the unique aspects of a digital modification (e.g., the possibility of a software CCF).

Sources of Results:

NEI 96-07, Section 4.3.6 states:

~~[3] Refer to NEI 96-07, Section 4.3.6, 4th paragraph.~~

Formatted: Highlight
Formatted: Highlight
Formatted: Highlight
Formatted: Highlight
Formatted: Highlight

> "*Attention must be given to whether the malfunction was evaluated in the* ***accident analyses*** *at the component level or the overall system level.*" [***emphasis*** added]

Accident analyses are typically included and described in UFSAR Chapters 6 and 15 (or equivalent).

The phrase "was evaluated in the accident analyses" refers to how the malfunction was addressed in the accident analysis (e.g., failure to perform a design function, failure to cease performing a design function, etc.) and the level at which the malfunction was addressed in the accident analysis (e.g., component, train, system, etc.).

Types of Results:

In NEI 96-07, Section 4.3.6, the second bullet/example after the first paragraph states:

> "*If a feedwater control system is being upgraded from an analog to a digital system, new components may be added that could fail in ways other than the components in the original design. Provided the* ***end result*** *of the component or subsystem failure is the same as, or is bounded by, the results~~...~~ of malfunctions currently described in the UFSAR (i.e., failure to maximum demand, failure to minimum demand, failure as-is, etc.)~~...~~, then~~...~~[the activity]~~...~~ would not create a 'malfunction with a different result'*." [***emphasis*** added]

Many types of *results* can be described in a UFSAR. The focus on the *end result* implies the effect of the failure mode is what is important not the failure mechanism~~the possible existence of other *non-end results*. For clarity, all results other than the *end result* will be identified as *intermediate results*. No *intermediate results* need to be considered.~~

As a general example, consider the following possible levels of malfunction results that could be described in a UFSAR:

- Failure Mechanism - new failure mechanisms for existing failure modes do not produce different results

- Failure Mode - new failure modes need to be evaluated to determined whether their effect is a different result

- ~~Component Level Result~~

Commented [A89]: Source: NEI 96-07 Page 54. Rational: Complete quotation is needed so that intent is cearly understood.

Commented [A90]: Source: NEI 96-07 Page 54. Rationale: Intent of quotation is clarified.

- ~~System Level Result (from the component level malfunction)~~
- ~~Plant Level Result (from the system level malfunction)~~

~~In this generalized example, the Component Level and System Level results would be considered *intermediate results* and the Plant Level result would be considered the *end result*. Only the Plant Level result is pertinent and needs to be considered when determining if the possibility of a malfunction with a different result has been created.~~

Commented [A91]: Source: NEI 96-07 Page 54.
Rationale: Intent of quotation is clarified.

Example 4-22 illustrates the ~~NO~~ CREATION of the possibility of a malfunction with a different result case.

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

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

A malfunction identified in the UFSAR for the analog main feedwater control systems involves the loss of one main feedwater pump (out of two pumps), which is evaluated in the Loss of Feedwater accident analysis.

Credible Conclusion

Formatted: Highlight

Based on the technical outcome from the CCF Susceptibility Analysis and the Failure Modes and Effects Analysis (FMEA) performed as part of the technical assessment supporting this digital modification, a software CCF impacting both feedwater control systems has been determined to be credible.

Formatted: Highlight

Bounded Conclusion

Types of Malfunctions:

A CCF can cause the loss of <u>both</u> main feedwater pumps.

Source of Result:

Currently, the malfunction of the MFWP is evaluated to "stop" and the malfunction is evaluated at the component level (i.e., the "pump" is assumed to stop).

Assuming the CCF occurs, the malfunction will continue to be evaluated as the "stopping" of MFWPs and the level of the malfunction remains at the component level (i.e., the "pump").

Type of Result:

The UFSAR identifies the malfunction of one main feedwater pump as causing a reduction in flow (~~intermediate result~~<u>mode & effect</u>) to the steam generators, which initiates a Loss of Feedwater event~~ (end result)~~.

The loss of both main feedwater pumps causes <u>no</u> flow to the steam generators ("new" ~~intermediate~~ <u>mode & effect</u>~~result~~), which still initiates the Loss of Feedwater event~~ ("new" end result);~~<u>therefore,</u>~~.~~ <u>a loss of feedwater accident analysis should be performed to determine whether any of the limiting criteria have been exceeded.</u>

In both instances, the end result is the Loss of Feedwater event.

<u>Overall Conclusion</u>

~~Although t~~<u>T</u>he impact of the ~~intermediate~~ result on the accident analysis acceptance criteria is most likely more severe (by going from the loss of <u>one</u> pump to the loss of <u>both</u> pumps), the result of the CCF is <u>NOT</u> bounded. Therefore, the proposed activity does ~~NOT~~ create the possibility of a malfunction with a <u>different</u> result.

Commented [A92]: Incorrectly implies that a "different result" is limited to plant level accident analysis results which is contrary to 50.59(c)(2)(viii) which states "different result than ANY previously evaluated malfunctions" which includes UFSAR described FMEAs for the affected system.

Example 4-23 illustrates the CREATION of the possibility of a malfunction with a different result case.

Example 4-23. CREATION of the Possibility of a Malfunction with a Different Result

Proposed Activity

Two non-safety-related analog feedwater control systems and a separate analog control system that controls the main turbine steam-inlet valves exist.

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

Malfunction / Accident

From the UFSAR, 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 accident analysis] and (b) failures causing an increase in main feedwater flow to the maximum output from both MFWPs [evaluated in the Excess Feedwater accident analysis].

From the UFSAR, 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 accident analysis] and (b) all valves going fully open causing excess steam to be admitted into the turbine [evaluated in the Excess Steam Demand accident analysis].

Credible Conclusion

Formatted: Highlight

Based on the technical outcome from the CCF Susceptibility Analysis and the Failure Modes and Effects Analysis (FMEA) performed as part of the technical assessment supporting this digital modification, a software CCF impacting the feedwater control systems and the main turbine steam-inlet valve control system has been determined to be credible.

Formatted: Highlight

Bounded Conclusion

Types of Malfunctions:

A CCF can cause any of following conditions:

(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)

Source of Result:

Currently, the malfunctions are evaluated as affecting only one system (i.e., feedwater control or main turbine control, NOT both) and the malfunctions are evaluated at the component level (i.e., "pump" or "valve").

Assuming the CCF occurs, the malfunction will no longer affect only one system, but will continue to be evaluated at the component level (i.e., "pump" or "valve").

Type of Result:

The UFSAR identifies the end result of a malfunction as causing a Feedwater event or a Main Steam event, NOT both.

In Conditions (5) through (8), the end result is no longer a Feedwater event or a Main Steam event.

Overall Conclusion

Based on the current set of accidents identified in the UFSAR, the accident analyses do not consider a simultaneous Feedwater/Main Steam event.

The different results [simultaneous accidents in Conditions (5) though (8)] are NOT *bounded* by the previously-evaluated results of only one accident. Therefore, the proposed activity does create the possibility of a malfunction with a different result.

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]

Page 37: [1] Commented [A44] **Author**

Source: Engineering Judgement

Rationale: There are two things of concern:

(1) Determination of if CCF is credible

(2) Characterisation of behavior during CCF

Both could be considered outcomes; therefore this change was made to clarify the Outcomes being considerd in this section.