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

NEI 96-07, Appendix D
Draft Revision 0c

Commented [A1]: The NRC has formally provided comments to NEI regarding the screening section (ML17006A341), not all of which have been addressed in this document; specifics are provided in the comments below.

Nuclear Energy Institute

SUPPLEMENTAL GUIDANCE FOR APPLICATION OF 10 CFR 50.59 TO DIGITAL MODIFICATIONS

May 2017

DRAFT NRC Comments included for the purpose of discussion at the June 21, 2017 Public Meeting.

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

DRAFT NRC Comments included for the purpose of discussion at the June 21, 2017 Public Meeting.

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 2

1.2 PURPOSE 3

2 [NOT USED] 3

3 DEFINITIONS AND APPLICABILITY OF TERMS 3

4 IMPLEMENTATION GUIDANCE 4

4.1 APPLICABILITY 4

4.2 SCREENING 4

4.3 EVALUATION PROCESS 23

5.0 EXAMPLES 54

1 INTRODUCTION

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 separating technical guidance from 10 CFR 50.59 related guidance.

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

Commented [A2]: This paragraph and associated concept is incomplete. The section does not specifically state NEI's plan, regarding Appendix D and NEI 16-16, which is to replace the complete guidance of NEI 01-01. The paragraph also gives the impression that NEI 16-16 replaces the technical guidance of NEI 01-01 when that has not been verified.

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 [A3]: This reference should be enhanced by describing specifically how NEI 16-16 can be used for Appendix D Screenings and Evaluations 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 modifications or replacements of mechanical or electrical equipment if the new equipment makes use of digital technology (e.g., a new HVAC design that includes embedded microprocessors for control).

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

2 [NOT USED]

This section is not used for digital modifications.

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.

Commented [A4]: By letter dated November 5, 2013 (see item 1 in the Enclosure) the NRC expressed concerns with terms in NEI 01-01.

By letter dated March 16, 2017 (ML17006A341), in Comment No. 12, the NRC stated that new terms should be defined.

There are new terms that are used in this document (e.g., CCF Susceptibility Analysis), but they are not defined. Provide definitions for all new terms added in subsequent revisions in draft Appendix D.

4 IMPLEMENTATION GUIDANCE

4.1 APPLICABILITY

There is no Applicability guidance unique to digital modifications.

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."

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.

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

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

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 [A5]: By letter dated March 16, 2017 (ML17006A341), in Comment No. 4, the NRC stated that the guidance under NEI 96-07 Rev. 1 Section 4.2.1.2 addresses the method of performing or controlling a design function.

This quotation and associated material show the NRC comment has not yet been addressed.

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 [A6]: Please delete. This information is not needed and is misleading (i.e., technically inaccurate).

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

Commented [A7]: By letter dated November 5, 2013 (see item 10 in the Enclosure) the NRC expressed concerns with introduced interactions or couplings.

By letter dated March 16, 2017 (ML17006A341), in Comment No. 14, the NRC stated that additional considerations were necessary.

Coupling mechanisms should be explicitly addressed (e.g., digital communications). See also ML16358A153:
"An important aspect of ensuring defense-in-depth is to guard against CCF. Failure of multiple components to function may occur as a result of a single specific cause or event that could simultaneously affect several components important to risk. The cause or event may include an installation or construction deficiency, accidental human action, extreme external environment, or an unintended cascading effect from any other operation or failure within the plant. CCFs can also result from poor design, manufacturing, or maintenance practices.

To defend against CCF, 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. Coupling factors can be based on, but may not necessarily be limited to the following attributes…"

USE OF SOFTWARE AND DIGITAL DEVICES

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

Commented [A8]: By letter dated March 16, 2017 (ML17006A341), in Comment No. 9, the NRC addressed providing guidance which implies exclusion of indirect effects.

The addition of the phrase "described in the FSAR" seems to allow a change in the intent of the rule, as stated in the statements of consideration (and NEI 96-07 Rev. 1 Section 4.2.1.):
"The Commission considered these comments in selecting the language that allows screening as to whether a change to the facility affects the content of the FSAR. As previously noted in implementation guidance, some SSC or subcomponents may not be explicitly described in the FSAR, but they have the potential to affect the function of an SSC that is described. The approach chosen by the Commission for defining "change" as relating to those additions, modifications, and removals that affect functions, methods of performing or controlling functions and evaluation methods also accomplishes an important purpose for these issues. Some changes a licensee may wish to make to a component or procedure could affect the functions or performance requirements of other SSC. Depending upon the level of detail contained in the FSAR, the particular component being changed may not be explicitly described. If a modification to that (non-described) component could affect any SSC design function or performance requirements that are described, that modification affects the design function, and thus is a change as defined by § 50.59(a) and thus requires evaluation under § 50.59."

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

An adverse effect may also consist of the potential marginal increase in the likelihood of SSC failure due to the introduction of software. For redundant safety systems, this marginal increase in likelihood creates a similar marginal increase in the likelihood of a common failure in the redundant safety systems. On this basis, most digital modifications to redundant safety systems are *adverse*. However, for some digital modifications, engineering evaluations may show that the digital modification contains design attributes

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

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*.

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.

Commented [A9]: What example clatifies this guidance?

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

Commented [A10]: This Example and the text preceding it (as well as the Examples in general) appear to perpetuate the concern described in Item 1) in the Enclosure of the November 5, 2013 letter from NRC to NEI regarding concerns with NEI 01-01. Specifically, Example 5.1 from NEI 01-01. The concern notes that the complexity of the new internal software is ignored in Example 5.1 with the focus being only on the inputs and outputs. The approach in general of this App. D seems to be to ignore the internal differences of new digital system as compared to the old analog control system. The NRC staff continues to have concerns with this approach.

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.

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 functions 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 functions 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 since the UFSAR does not describe SSCs for the purpose of establishing defense-in-depth and there are no UFSAR-described design functions 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.

Commented [A11]: By letter dated March 16, 2017 (ML17006A341), in Comment No. 9, the NRC addressed providing guidance which implies exclusion of indirect effects. This comment was not fully addressed.

From this explanation, readers may abstract the following guidance: In order for there to be no reduction in Redundancy, two conditions must simultaneously be met: (1) the UFSAR must not describe redundant SSCs, and (2) there are no UFSAR-Described design functions related to redundancy.

However, this abstraction ignores indirect effects.

Commented [A12]: NRC staff recommends deleting this clause as it is contrary to the corresponding guidance in NEI 96-07 because mentioning "UFSAR" description eliminates consideration of "indirect effects."

If the UFSAR does not specifically discuss "redundancy," "diversity," or "defense-in-depth," an activity that reduces the actual physical existing redundancy, diversity or defense-in-depth could still have an adverse effect on the design function. In addition, this example omits the newly added Appendix D guidance, Section 4.2.1.1,, "An adverse effect may also consist of the potential marginal increase in the likelihood of SSC failure due to the introduction of software. For redundant safety systems, this marginal increase in likelihood creates a similar marginal increase in the likelihood of a common failure in redundant safety systems. On this basis, most digital modifications to redundant safety systems are adverse."

Commented [A13]: Generally, UFSARs contain very few (if any) "descriptions of SSCs for the purpose of establishing defense-in-depth;" however, there was a very significant amount of consideration of defense-in-depth is establishing regulatory requirements and in approving applications.

Effectively the guidance provided in this examples can be understood to say "if there is no explicit discussion of defense-in-depth with respect to a SSC, in the UFSAR" there is no potential to adversely impact the defense-in-depth of the facility.

Please provide an appropriate "Defense-in-Depth Consideration."

Commented [A14]: By letter dated March 16, 2017 (ML17006A341), in Comment No. 4, the NRC stated that the guidance under NEI 96-07 Rev. 1 Section 4.2.1.2 addresses the method of performing or controlling a design function.

This quotation and associated material show the NRC comment has not been addressed.

In NEI 96-07, this phrase is used to refer to what an operator does, not to how equipment works. This example does not talk at all about impact on the operator, so this conclusion phrase is out of context.

Please delete this phrase.

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.

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, 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 the SSC's ability or capability of performing 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 assist in determining the impact of a digital modification on the number and/or arrangement of components, review the description(s) of the existing

Commented [A15]: By letter dated March 16, 2017 (ML17006A341), in Comment No. 14, the NRC recommended adding the following words (from NEI 01-01 Section 4.3.3):

"In addition to the software question, other characteristics of a digital upgrade could cause the change to screen in to a 10 CFR 50.59 evaluation. Some potentially adverse effects that should be evaluated when screening digital upgrades include:
•Combining previously separate functions into one digital device such that failures create new malfunctions (i.e., multiple functions are disabled if the digital device fails).
•Changing performance from UFSAR-described requirements (e.g., for response time, accuracy, etc.).
•Changing functionality in a way that increases complexity, potentially creating new malfunctions.
•Introducing different behavior or potential failure modes (for which the risk is not negligible) that could affect the design function."

These words were not added; therefore the NRC comment has not been addressed.

Commented [A16]: Please change to "a". This would prohibit a combination in one system from adversely affecting another system.

SSCs described in the UFSAR. 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.

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 all feedwater to the steam generators, and

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

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

SCOPE

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.

Commented [A17]: By letter dated March 16, 2017 (ML17006A341), in Comment No. 18, the NRC stated that non-HSI changes can have adverse impacts on the operator that must be evaluated. This comment has not been addressed.

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

Commented [A18]: By letter dated March 16, 2017 (ML17006A341), in Comment No. 19, the NRC stated that additional considerations were necessary. This comment has not been addressed.

By letter dated March 16, 2017 (ML17006A341), in Comment No. 26, the NRC stated that additional considerations were necessary. This comment has not been addressed.

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.

Examples 4-5 through 4-7 illustrate the application of the *Physical Interaction* aspect.

Example 4-5. Physical Interaction with NO ADVERSE IMPACT on a UFSAR-Described Design Function

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.

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).

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.

Using the results from the HFE and examining only the physical interaction aspect (e.g., ignoring the impact on operator response time or the number

Commented [A19]: By letter dated March 16, 2017 (ML17006A341), in Comment No. 22, the NRC stated that it is inappropriate to base HSI adversity determinations based on UFSAR description of the HSI, since there generally were none. This comment has not been addressed.

Example is not adequate to screen or evaluate for HSI impacts. Plant UFSARs were not typically developed with HSI considerations such that a broad HSI assessment is required to properly screen and evaluate proposed changes. The example provided is too limited and unrealistic to provide adequate guidance for HSI assessments. NRC recommends removing the example or revising it to provide the broader HSI assessment considerations required for an adequate HSI assessment.

and/or sequence of steps necessary to access the new digital controls), 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.

Commented [A20]: Example is not adequate to screen or evaluate for HSI impacts. Plant UFSARs were not typically developed with HSI considerations such that a broad HSI assessment is required to properly screen and evaluate proposed changes. The example provided is too limited and unrealistic to provide adequate guidance for HSI assessments. NRC recommends removing the example or revising it to provide the broader HSI assessment considerations required for an adequate HSI assessment.

In fact this guidance may make things worse, since it implies that if it is not described in the UFSAR, then no changes to it can be adverse.

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.

Commented [A21]: Example is not adequate to screen or evaluate for HSI impacts. Plant UFSARs were not typically developed with HSI considerations such that a broad HSI assessment is required to properly screen and evaluate proposed changes. The example provided is too limited and unrealistic to provide adequate guidance for HSI assessments. NRC recommends removing the example or revising it to provide the broader HSI assessment considerations required for an adequate HSI assessment.

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.,

Commented [A22]: Example is not adequate to screen or evaluate for HSI impacts. Plant UFSARs were not typically developed with HSI considerations such that a broad HSI assessment is required to properly screen and evaluate proposed changes. The example provided is too limited and unrealistic to provide adequate guidance for HSI assessments. NRC recommends removing the example or revising it to provide the broader HSI assessment considerations required for an adequate HSI assessment.

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."

Commented [A23]: Example is not adequate to screen or evaluate for HSI impacts. Plant UFSARs were not typically developed with HSI considerations such that a broad HSI assessment is required to properly screen and evaluate proposed changes. The example provided is too limited and unrealistic to provide adequate guidance for HSI assessments. NRC recommends removing the example or revising it to provide the broader HSI assessment considerations required for an adequate HSI assessment.

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.

Commented [A24]: Example is not adequate to screen or evaluate for HSI impacts. Plant UFSARs were not typically developed with HSI considerations such that a broad HSI assessment is required to properly screen and evaluate proposed changes. The example provided is too limited and unrealistic to provide adequate guidance for HSI assessments. NRC recommends removing the example or revising it to provide the broader HSI assessment considerations required for an adequate HSI assessment.

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.

Commented [A25]: Example is not adequate to screen or evaluate for HSI impacts. Plant UFSARs were not typically developed with HSI considerations such that a broad HSI assessment is required to properly screen and evaluate proposed changes. The example provided is too limited and unrealistic to provide adequate guidance for HSI assessments. NRC recommends removing the example or revising it to provide the broader HSI assessment considerations required for an adequate HSI assessment.

- 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 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 design function 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.

Commented [A26]: By letter dated March 16, 2017 (ML17006A341), in Comment No. 25, the NRC stated that the absence of UFSAR described response time does not constitute "No response time requirements". This comment has not been addressed.

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.

Commented [A27]: See old comment No. 25 Comment above.

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.

In the following sections and sub-sections that describe the Evaluation guidance unique to 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."

Common Cause Failure (CCF) Outcomes

The possible outcomes regarding a CCF from the CCF Susceptibility Analysis performed in accordance with applicable Industry and/or NRC guidance documents are as follows:

(1) CCF not credible (i.e., likelihood of a CCF caused by an I&C failure source is NOT greater than the likelihood of a CCF caused by other failure sources that are not considered in the UFSAR)

(2) CCF credible (i.e., likelihood of a CCF caused by an I&C failure source IS greater than or equal to the likelihood of a CCF caused by other failure sources that are considered in the UFSAR)

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

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.

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...*"

Commented [A28]: Re-insert "NRC-endorsed"

Commented [A29]: There are no NRC guidance documents for "CCF Susceptibility" or "CCF not credible"

Commented [A30]: CCF likelihood "greater than" or "Less than or equal to" inappropriately implies the technical capability that does not exist. Use 01-01 which states "comparable to CCF not described"

Commented [A31]: NEI 96-07r1 states that, for and analog to digital upgrade, CCF is "credible" so guidance (that clarifies NEI 96-07r1) should not conflict with this position.

Presumably these terms (i.e., CCF Credible or not) are used to align with NEI 16-16. It is understood that NEI 16-16 can be used for both license amendment requests (LARs) and under the 50.59 process; however, the SRP guidance also does not use the distinction between CCF Credible or not. So in this respect NEI 16-16 does not align with either SRP or 50.59 guidance.

NEI 01-01 reaches a conclusion that CCF likelihood is "Sufficiently Low." In the Qualitative Assessment, "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).
- NEI 96-07r1/NEI 01-01/50.59 describe no 50.59 screening or evaluation decisions based on "credible," only "likelihood."
- A Qualitative Assessment of "likelihood" is needed to address other criteria anyway (e.g., 50.59 Criterion ii "likelihood of a malfunction").

Commented [A32]: NEI 01-01 reaches a conclusion CCF Likelihood "Sufficiently Low" (In the Qualitative Assessment, "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).
- NEI 96-07r1 and NEI 01-01 both state that a CCF for and analog to digital upgrade is "credible" so an NEI 16-16 determination otherwise creates unnecessary confusion.
- NEI 96-07r1/NEI 01-01/50.59 describe no 50.59 screening or evaluation decisions based on "credible," only "likelihood."
- A Qualitative Assessment of "likelihood" is needed to address other criteria anyway (e.g., 50.59 Criterion ii "likelihood of a malfunction") which allows for one Qualitative Assessment.

Commented [A33]: There should be examples beyond MFW, such as safety auxiliary systems, and other types of modifications more representative of the types of digital upgrades happening across industry. Does NEI intend to place more examples of varying degrees of complexity into Section 5? The Appendix D team should consider working closely with the NEI 16-16 team to ensure that examples provide a wide range of SSC examples. Especially SSCs whose specific malfunction is not explicitly described in the safety analyses.

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 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 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 guidance described in NEI 96-07, 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 an accident frequency are not available, so the qualitative approach using the *attributable* and the magnitude (i.e., *negligible/discernable*) criteria from NEI 96-07, Section 4.3.1 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 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.

Commented [A34]: Change to "SW CCF." There have been many documented CCFs in the nuclear industry (see NUREG/CR-6268 & NUREG/CR-6813), and they were not just in digital systems.

Commented [A35]: This type of argument would generally be considered acceptable; however, there is no specific guidance in NEI 96-07 Section 4.3.1 relating to a SSCs compatibility with the environment.

There are three general pieces of guidance that could be applied to environmental compatibility:
(1) "Although this criterion allows minimal increases, licensees must still meet applicable regulatory requirements and other acceptance criteria to which they are committed (such as contained in regulatory guides and nationally recognized industry consensus standards, e.g., the ASME B&PV Code and IEEE standards)." This guidance is only appropriate if there are necessary and sufficient "applicable regulatory requirements and other acceptance criteria to which they are committed," otherwise a necessary and sufficient set must be established.
(2) "Further, departures from the design, fabrication, construction, testing and performance standards as outlined in the General Design Criteria (Appendix A to Part 50) are not compatible with a "no more than minimal increase" standard." This guidance is appropriate for establishing the necessary and sufficient set of criteria to which a new technology or system design must conform. Obviously, current RGs and endorsed Standard are an acceptable way to meet this guidance. Alternatively, stipulated criteria or other standards may also be acceptable; does industry feel this alternative (for digital technology and systems) has sufficiently low regulatory uncertainty so no additional guidance in this area is required?
(3) "The proposed activity meets applicable NRC requirements as well as the design, material and construction standards applicable to the SSC being modified. If the proposed activity would not meet applicable requirements and standards, the change is considered to involve more than a minimal increase in the frequency of occurrence of an accident, and prior NRC approval is required." The issues with this guidance are similar to those with the previous guidance.

Commented [A36]: NEI 96-07 does not describe how to perform qualitative assessments; NEI 01-01 does, but that is to be superseded by Appendix D. Where will it be described how to perform a qualitative assessment for: attributable, discernable, and likelihood?

Commented [A37]: System and software design also have an impact on CCF frequency. That is, the high quality implementation of a poor design will result in a poor system, not a high quality system. It is technically inappropriate to ignore design attributes and focus solely on process attributes.

Commented [A38]: The guidance on Qualitative Assessment (i.e., RIS 2017-XX) provides a means of demonstrating the activity does not result in more than a minimal increase in the likelihood of failure of an SSC to important to safety perform its intended design functions described in the UFSAR and CCF Likelihood "Sufficiently Low" (In the Qualitative Assessment, "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) For proposed activities that affect SSCs whose failure could initiate an accident, the RIS 2017-XX Qualitative Assessment of the likelihood of failure, which corresponds to the frequency of failure, is an acceptable means of demonstrating, provides determination regarding the frequency of occurrence of an accident.

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

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

Digital components are expected to be more reliable than the equipment being replaced. Aspects to be addressed include the following: compliance with applicable regulations and industry standards; qualification for environmental conditions (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

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 frequency of an accident. 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).

Commented [A39]: There are two categories of things to consider:
(1) known threats, and
(2) unknown threats.

Design attributes are used to address (1) and process quality are used to address (2). For example digital communications between redundancies is a known vector for CCF, and a high quality development process, alone, is not adequate for addressing this vector.

Item 5. below should provide guidance to address (1).

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 Attributable

If a CCF is determined to be not credible, then there is NO *attributable* impact on the frequency of occurrence of an accident. Namely, if a CCF is 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 an accident initiator, then there is NO *attributable* impact on the frequency of occurrence of an accident. Namely, even if a CCF does occur, there is no relationship between the CCF and the accident initiator(s).

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

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

Commented [A40]: If a possible malfunction due to CCF is introduced by a change is determined to have a "sufficiently low" likelihood, this does not negate that the CCF is "attributable" to the change – it simply means there is no discernable increase in frequency.

Commented [A41]: If the component/system mitigates an accident, should guidance be provided for question 3?

Also should guidance be provide for malfunction mitigator under questions 3 & 4?

Commented [A42]: These chillers are accident mitigators. How would this example work under Questions 3 & 4?

same supplier and the software in each digital control system is exactly the same.

Affected Accidents and Accident Initiators

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

Impact on Accident Frequency

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; after the accidents have already occurred. Therefore, there is NO impact on the frequency of occurrence of the accidents that can be *attributed* to the digital modification.

Commented [A43]: Please provide an example that addresses the potential impact on the consequences under questions 3 & 4.

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 credible.

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.

Commented [A44]: It seems like the more applicable criteria, based on the yellow highlighting above, for this example would be consequences, or new type?

Determination of Magnitude (using *Negligible/Discernable*)

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.

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 would NOT be more than minimal if applicable NRC requirements, as well as design, material, and construction standards, continue to be met.

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

Commented [A45]: NEI 96-07 says NOT meeting criteria means the increase is discernable. Also, most licensees have not "committed" to digital standards. Specifically, 4.3.1 states "Although this criterion allows minimal increases, licensees must still meet applicable regulatory requirements and other acceptance criteria **to which they are committed** (such as contained in regulatory guides and nationally recognized industry consensus standards, e.g., the ASME B&PV Code and IEEE standards). Further, departures from the design, fabrication, construction, testing and performance standards as outlined in the General Design Criteria (Appendix A to Part 50) are not compatible with a "no more than minimal increase" standard."

In summary meeting criteria is necessary, but not sufficient justification for performing a design modification under 50.59.

Commented [A46]: NEI 96-07 says NOT meeting criteria means the increase is discernable. This wording seems to say meeting said criteria is necessary and sufficient to conclude "not discernable," however, there are other reason that the increase could be discernable.

These ambiguities revolve around the human tendency to think of things in a binary fashion, were in actuality thigs may not be so. That is, not meeting NRC regulatory requirements, should be treated as a discernable increase, while meeting regulatory requirements may or may not result in a discernable increase.

The point is that there are two types of requirements: (1) general, and (2) functionally specific. The NRC's regulatory requirements generally aggregates general process or product aspects; it is possible to meet all of these, and the design could by less reliable. This idea is most apparent in the consequences questions. For example, a larger pipe could be installed in accordance with all regulatory requirements, but the failure of this larger pipe could still produce a more than a minimal increase in the consequences of the accident or malfunction.

In the area of reliability, there may be different coincidences systems that all meet regulatory requirements:
(1) One out of Two
(2) Two out of Three
(3) Two out of Four
(4) One out of two taken twice
However, assuming comparable equipment reliability, they each have a discernibly different reliabilities.

The point is systems design and regulatory requirements must both be considered.

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.

Commented [A47]: This seems to look at the criteria backwards. This implies one must be able to prove the system is less reliable, for it to fail 50.59. As opposed to proving the system is more reliable in order to be able to pass. For first of a kind systems, it is hard to prove any sort of "clear trend".

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.

Commented [A48]: NEI 96-07 Section 4.3.1 states "Although this criterion allows minimal increases, licensees must still meet applicable regulatory requirements and other acceptance criteria to which they are committed (such as contained in regulatory guides and nationally recognized industry consensus standards, e.g., the ASME B&PV Code and IEEE standards). Further, departures from the design, fabrication, construction, testing and performance standards as outlined in the General Design Criteria (Appendix A to Part 50) are not compatible with a "no more than minimal increase" standard."

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.

Commented [A49]: This section, in addition to one very similar section under Questions 2, is the only HSI evaluation guidance.

Why is there no similar guidance for the other questions?

It is not clear how to apply the "qualitative evaluation guidance" to the HSI domain.

It is not clear how to map attributable or discernable to HRA analyses.

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 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 [A50]: Replace with "SW CCF."

Maybe "SW CCF" could be defined for this document as "unknown unknowns" and all known CCF vectors get referred to explicitly.

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.

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.

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).

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

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 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 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).

Commented [A51]: If a possible malfunction due to CCF is introduced by a change is determined to have a "sufficiently low" likelihood, this does not negate that the CCF is "attributable" to the change – it simply means there is no discernable increase in frequency

Commented [A52]: Malfunction mitigators should be addressed in Question 4.

Commented [A53]: NEI 96-07r1 does not use the term "malfunction initiator", only "accident initiator" "transient initiator" because 50.59 involves any malfunctions that can affect a design function, not simply malfunctions already described in the UFSAR. NRC Staff recommend deleting all text related to malfunction initiators.

Commented [A54]: Example is not adequate to screen or evaluate for HSI impacts. Plant UFSARs were not typically developed with HSI considerations such that a broad HSI assessment is required to properly screen and evaluate proposed changes. The example provided is too limited and unrealistic to provide adequate guidance for HSI assessments. NRC recommends removing the example or revising it to provide the broader HSI assessment considerations required for an adequate HSI assessment.

Commented [A55]: NRC staff recommends removing "UFSAR identifies" because it incorrect limits consideration to what is explicitly described in the UFSAR. In determining whether there is more than a minimal increase in the likelihood of occurrence of a malfunction of an SSC to perform its design function as described in the UFSAR, the first step is to determine what SSCs are affected by the proposed activity. Next, the effects of the proposed activity on the affected SSCs should be determined. This evaluation should include both direct and indirect effects. Direct effects are those where the proposed activity affects the SSCs (e.g., a motor change on a pump). Indirect effects are those where the proposed activity affects one SSC and this SSC affects the capability of another SSC to perform its UFSAR-described design function. Indirect effects also include the effects of proposed activities on the design functions of SSCs credited in the safety analyses. The safety analysis assumes certain design functions of SSCs in demonstrating the adequacy of design. Thus, certain design functions, while not specifically identified in the safety analysis, are credited in an indirect sense.

Commented [A56]: NEI 96-07 does NOT limit consideration of an increase in likelihood to only explicit UFSAR described components/malfunctions. Also, malfunctions are generally described in the UFSAR a postulated single failures, and thus any single failure malfunction is considered previously evaluated. Which means any postulated single failure not just the specific single failure malfunctions explicitly described in the UFSAR. The following sentence from NEI 96-07 section 4.3.2 describes new components and new malfunctions confirming that Criterion ii is not limited to an increase in likelihood of the specific UFSAR described malfunctions "Thus, for instance, if failures were previously postulated on a train level because the trains were independent, a proposed activity that introduces a cross-tie or credible common mode failure (e.g., as a result of an analog to digital upgrade) should be evaluated further to see whether the likelihood of malfunction has been increased."

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, there is NO impact on the likelihood of occurrence of the malfunction that can be *attributed* to the digital modification.

Commented [A57]: This logic is fundamentally flawed.

The items described in the FSAR, may be the most dominate (or probable) cause, but NOT the only causes of a malfunction!

ANY design change that causes a significant increase in the likelihood of a malfunction should failure this question (whether or not this source is described in the SAR)!

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.

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

Commented [A58]: Example is not adequate to screen or evaluate for HSI impacts. Plant UFSARs were not typically developed with HSI considerations such that a broad HSI assessment is required to properly screen and evaluate proposed changes. The example provided is too limited and unrealistic to provide adequate guidance for HSI assessments. NRC recommends removing the example or revising it to provide the broader HSI assessment considerations required for an adequate HSI assessment.

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.

Commented [A59]: Specific UFSAR wording is not a consideration.

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.

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.

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.

Example 4-18 illustrates the NEGLIGIBLE impact case.

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

Commented [A60]: Example is not adequate to screen or evaluate for HSI impacts. Plant UFSARs were not typically developed with HSI considerations such that a broad HSI assessment is required to properly screen and evaluate proposed changes. The example provided is too limited and unrealistic to provide adequate guidance for HSI assessments. NRC recommends removing the example or revising it to provide the broader HSI assessment considerations required for an adequate HSI assessment.

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

Commented [A61]: "Discernable" may be a better choice.

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 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.

Commented [A62]: How is a clear trend demonstrated for a first of a kind design?

Example 4-19 illustrates the DISCERNABLE increase case.

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

Commented [A63]: Example is not adequate to screen or evaluate for HSI impacts. Plant UFSARs were not typically developed with HSI considerations such that a broad HSI assessment is required to properly screen and evaluate proposed changes. The example provided is too limited and unrealistic to provide adequate guidance for HSI assessments. NRC recommends removing the example or revising it to provide the broader HSI assessment considerations required for an adequate HSI assessment.

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."

Commented [A64]: Incorrectly indicates the 50.59 decision is limited to the likelihood of malfunctions already described in the UFSAR. Contrary to the corresponding guidance in NEI 96-07 because mentioning "UFSAR" description eliminates consideration of "indirect effects."

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

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.

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

Commented [A65]: What about unidentified sources?

Where/ how identified?

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?

INTRODUCTION

From NEI 96-07, Section 3.2:

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

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

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

Commented [A66]: Why is there no HSI guidance for this section?

For example, if a new capability to control is created, then is not a new capability to miss-control created?

Commented [A67]: RG 1.187 is being revised to clarify that an accident of a new type is an accident that is:
(1) Related and unbounded, or
(2) Not related
to existing accident types.

add "unrelated" to consideration because an accident of a different type also means a new accident analysis is needed so being bounded by existing analyses is not a consideration.

GUIDANCE

Determination of Credible

If a CCF is determined to be not credible, 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]

Commented [A68]: Same comment as for Criterion i regarding "credible" and the RIS 2017-XX Qualitative Assessment.

If a CCF is determined to be credible, 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 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 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 meets the *bounded* criterion. Alternately, a new accident that is NOT of the same type (i.e., its effect on the plant is different) and/or is NOT within the same expected frequency of occurrence does NOT meet the *bounded* criterion.

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

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

evaluated in the UFSAR. Namely, a **different/new** accident analysis would be needed for this different type of accident, not just 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.

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 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 *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 create the possibility of an accident of a different type.

Commented [A69]: Same analysis, but more adverse inputs and therefore unbounded outputs, should require a LAR.

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

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

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.

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

(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?

Commented [A70]: Why is there no HSI guidance for this section?

For example, if a new capability to control is created, then is not a new capability to miss-control created?

INTRODUCTION

From NEI 96-07, Section 4.3.6, the two considerations that need to be assessed when answering this question are *credible* and *bounded*.

Commented [A71]: Same comment as for Criterion i regarding "credible" and the RIS 2017-XX Qualitative Assessment.

GUIDANCE

Determination of Credible

If a CCF is determined to be not credible, then the creation of a possibility for a malfunction with a different result is NOT *credible* 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 is determined to be credible, then the creation of a possibility for a malfunction with a different result is *credible*.

Determination of Bounded

Commented [A72]: Is the guidance in NEI 16-16 with regards to bounding fully compatible with the guidance that is stated in section 4.3.6 of this draft of Appendix D? If not, what portions of NEI 16-16's bounding guidance is applicable here and which portions are not?

For the case in which a CCF is credible, 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:

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

> "*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:

> "*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:

> "*Provided the **end result** of the component or subsystem failure is the same as, or is bounded by, the results...described in the UFSAR..., 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*

Commented [A73]: End Result does NOT mean Plant Level.
NEI 96-07 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 this upgrade would not create a "malfunction with a different result.""
NEI 01-01 states, "
"Note that new types of malfunctions are not the issue. NEI 96-07, Revision 1, states that "a new failure mechanism is not a malfunction with a different result if the result or effect is the same as, or is bounded by, that previously evaluated in the UFSAR." As an example, NEI 96-07, Revision 1, notes that a digital feedwater control system upgrade may add new components that can have failure modes different than the original components. Provided the end result of the control system failure is bounded by the results of malfunctions already evaluated in the UFSAR (e.g., loss of feedwater), this upgrade would not create malfunctions with a different."

result implies 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:

- Component Level Result
- 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.

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.

Commented [A74]: What is the rationale that leads to the position that in all circumstances it is the plant level result (from the system level malfunction) is the "end result" of consideration. The above-quoted text, as well as subsequent guidance in Section 4.3.6 of NEI 96-07 does not appear to invoke the plant-level response. Only the response of the SSC at the level for which the malfunction was originally analyzed.

Commented [A75]: This framework appears to be a deviation from NEI 01-01 as NEI 01-01 does not currently have segregated levels of malfunction results. Please provide an explanation for how this framework aligns with NEI 01-01 or explain why this deviation was necessary.

Commented [A76]: If failures of the digital device cause the system to malfunction (i.e., not perform its design function), then the evaluation needs to determine if the result of the system malfunction is bounded by or different than those previously evaluated.

Commented [A77]: "The key issue is the **effect of failures of the digital device on the system in which it is installed**."
"Another way to determine the appropriate level of detail is to consider the level at which design functions are described in the UFSAR. If the relevant design functions are assigned at the system level, then it is appropriate to **evaluate the effects of malfunctions at this level.**"

NEI 96-07 never states or implies "bounded" is based on a plant level result.

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 impacting both feedwater control systems has been determined to be credible.

Bounded Conclusion

Types of Malfunctions:

A CCF can cause the loss of both 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) to the steam generators, which initiates a Loss of Feedwater event (end result).

The loss of both main feedwater pumps causes no flow to the steam generators ("new" intermediate result), which still initiates the Loss of Feedwater event ("new" end result).

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

Commented [A78]: The guidance must pick and consistently apply the same criteria. If the "result" is an event type as opposed to plant parameter values, then a CCF of control room chillers produces a different result.

How does one make a bounding determination based on event type? Bounding implies comparison of values.

Overall Conclusion

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

Commented [A79]: By what? Please explain!

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

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.

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.

Commented [A80]: Analysis seems to be based on qualitative evaluation of event type rather than quantitative based on plant parameter values. This is a change in conceptual approach.

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]