NEI 96-07, Appendix D
Draft Revision 0e

Nuclear Energy Institute

SUPPLEMENTAL GUIDANCE FOR APPLICATION OF 10 CFR 50.59 TO DIGITAL MODIFICATIONS

December 2017

ACKNOWLEDGMENTS

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

NOTICE

EXECUTIVE SUMMARY

NEI 96-07, Appendix D, *Supplemental Guidance for Application of 10 CFR 50.59 to Digital Modifications*, provides focused application of the 10 CFR 50.59 guidance contained in NEI 96-07, Revision 1, to activities involving digital modifications.

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

The guidance in this appendix supersedes the 10 CFR 50.59-related guidance contained in NEI 01-01/ EPRI TR-102348, Guideline on Licensing of Digital Upgrades.

TABLE OF CONTENTS

1 INTRODUCTION

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

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

1.1 BACKGROUND

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

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

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

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

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 Controllers and Field Programmable Gate Arrays).

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

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

1.3 10 CFR 50.59 PROCESS SUMMARY

No additional guidance is provided.

1.4 APPLICABILITY TO 10 CFR 72.48

No additional guidance is provided.

1.5 CONTENT OF THIS GUIDANCE DOCUMENT

No additional guidance is provided.

2 DEFENSE IN DEPTH DESIGN PHILOSOPHY AND 10 CFR 50.59

No additional guidance is provided.

3 DEFINITIONS AND APPLICABILITY OF TERMS

Definitions 3.1 through 3.14 are the same as those provided in NEI 96-07, Rev. 1. Definitions specific to this appendix are defined below.

3.15 Sufficiently Low

Sufficiently low means much lower than the likelihood of failures that are considered in the UFSAR (e.g., single failures) and comparable to other common cause failures that are not considered in the UFSAR (e.g., design flaws, maintenance errors, and calibration errors).

4 IMPLEMENTATION GUIDANCE

4.1 APPLICABILITY

No additional guidance is provided.

4.2 SCREENING

CAUTION

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

Introduction

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

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

Digital-to-Digital Replacements and "Equivalency"

In NEI 96-07, Section 4.2.1.1, equivalent replacements are discussed. However, digital-to-digital changes may not necessarily be equivalent because the component/system behaviors, response time, failure modes, etc. for the new component/system may be different from the old component/system. All non-equivalent digital-to-digital replacements should utilize the guidance provided in this Appendix.

Guidance Focus

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

This focused approach is intended to concentrate on the particular aspect of interest and does not imply that the other aspects do not apply or could not

be related to the aspect being addressed. Initially, all aspects need to be considered, with the knowledge that some of them may be able to be excluded based on the actual scope of the digital modification being reviewed.

Example Focus

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

Human-System Interface Evaluations

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

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

Introduction

A 10 CFR 50.59 Evaluation is required for digital modifications that adversely affect design functions, or the methods used to perform or control design functions. There is no regulatory requirement for a proposed activity involving a digital modification to *default* (i.e., be mandatorily "forced") to an adverse conclusion.

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

- The introduction of software or digital devices.
- The replacement of software and/or digital devices with other software and/or digital devices.
- The use of a digital processor to "calculate" a numerical value or "generate" a control signal using software in place of using analog components.

- Replacement of hard controls (i.e., pushbuttons, knobs, switches, etc.) to operate or control plant equipment with a touch-screen.

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

Scope of Digital Modifications

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

NEI 96-07, Section 4.2.1.1 provides guidance for activities that involve "...an SSC design function..." or a "...method of performing or controlling a design function..." and Section 4.2.1.2 provides guidance for activities that involve "...how SSC design functions are performed or controlled (including changes to UFSAR-described procedures, assumed operator actions and response times)."

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

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

SCOPE

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

(a) Use of Software and Digital Devices

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

USE OF SOFTWARE AND DIGITAL DEVICES

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

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

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

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

For relatively simple digital modifications, engineering evaluations may be used to show that the digital modification would not adversely affect design functions; even for digital modifications that involve redundant components/systems.

To reach a screen conclusion of *not adverse* for relatively simple digital modifications, the degree of assurance needed to make that conclusion is based on considerations such as the following:

- Physical Characteristics of the Digital Modification
  - The change has a limited scope (e.g., replace analog transmitter with a digital transmitter that drives an existing instrument loop)
  - Uses a relatively simple digital architecture internally (simple process of acquiring one input signal, setting one output, and performing some simple diagnostic checks)
  - Has limited functionality (e.g., transmitters used to drive signals for parameters monitored)
  - Can be comprehensively tested (but not necessarily 100 percent of all combinations)
- Engineering Evaluation Assessments
  - The quality of the design processes employed
  - Single failures of the digital device are encompassed by existing failures of the analog device (e.g., no new digital communications among devices that introduce possible new failure modes involving separate devices)
  - Has extensive applicable operating history

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

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

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

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

Example 4-1 illustrates the application of the guidance for a relatively simple digital modification.

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

Proposed Activity Description

Transmitters are used to drive signals for parameters monitored by redundant ESFAS channels. The original analog transmitters are to be replaced with microprocessor-based transmitters. The change is of limited scope since the existing 4-20 mA instrument loop is maintained for each channel without any changes other than replacing the transmitter itself.

The digital transmitters are used to drive signals of monitored parameters and thus have limited functionality with respect to the Engineered Safety Features Actuation System (ESFAS) design function.

Design Function Identification

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

Screen Response

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

Failures of the new digital device are encompassed by the failures of the existing analog device in that there are no new digital communications among devices that introduce possible new failure modes involving multiple devices. The engineering evaluation of the digital device concluded that the digital system is sufficiently dependable, the conclusion of which is based on the quality of the design processes employed, and the operating history of the software and hardware used. In addition, based on the simplicity of the device (one input and two outputs), it was comprehensively tested. Further, substantial operating history has demonstrated high reliability in applications similar to the ESFAS application.

Therefore, the proposed digital modification is *not adverse* because the digital modification is relatively simple and the assessment of the considerations identified above has determined that the reliability of performing the design function is not reduced and no new malfunctions are created.

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

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

Proposed Activity Description

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

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

Design Function Identification

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

Screen Response

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

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

Proposed Activity Description

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

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

Design Function Identification

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

The UFSAR identifies the following MFWP control system malfunctions:

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

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

Screen Response

The digital modification associated with this proposed activity is not relatively simple, so the process for assessing relatively simple digital modifications could not be used. There is an *adverse* impact on the design function of the main feedwater control system because the use of the exact same software in both digital control systems creates a new malfunction that could impact both MFWPs due to a potential software CCF.

COMBINATION OF COMPONENTS/SYSTEMS AND/OR FUNCTIONS

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

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

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

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

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

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

Proposed Activity Description

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

Option #1: Within each control system, all of the analog subcomponents will be replaced with a single digital device that consolidates all of the components, sub-components and the functions associated with each component and sub-component. The components in each analog control system will be replaced with a separate digital control system.

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

Design Function Identification

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

The UFSAR identifies the following MFWP control system malfunctions:

(a) failures causing the loss of all feedwater to the steam generators, and

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

Screen Response

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

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

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

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

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

Proposed Activity Description

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

Both analog controllers will be replaced with a single digital device that will perform in accordance with the original design requirements providing both temperature monitoring/control and air damper control.

Design Function Identification

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

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

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

Screen Response

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

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

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

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

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

to the combination aspect.

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

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

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

Proposed Activity Description

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

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

Design Function Identification

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

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

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

Screen Response

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

4.2.1.2 Screening of Changes to Procedures as Described in the UFSAR

SCOPE

If the digital modification does not include or affect a Human-System Interface (e.g., the replacement of a stand-alone analog relay with a digital relay that has no features involving personnel interaction and does not feed

signals into any other analog or digital device), then this section does not apply and may be excluded from the Screen assessment.

In NEI 96-07, Section 3.11 defines *procedures* as follows:

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

Although UFSARs do not typically describe the details of a specific Human-System Interface (HSI), UFSARs will describe any design functions associated with the HSI.

Because the HSI involves system/component operation, this portion of a digital modification is assessed in this Screen consideration. The focus of the Screen assessment is on potential adverse effects due to modifications of the interface between the human user and the technical device.

Note that the "human user" could involve Control Room Operators, other plant operators, maintenance personnel, engineering personnel, technicians, etc.

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

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

Any user of the HSI must be able to accurately perceive, comprehend and respond to system information via the HSI to successfully complete their tasks. Specifically, nuclear power plant personnel perform "four generic primary tasks" (Reference: NUREG/CR-6947):

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

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

Table 1 - Example Human-System Interface Modifications

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

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

- Step One - Identify the generic primary tasks that are involved with (i.e., potentially impacted by) the proposed activity.

- Step Two - For all primary tasks involved, assess if the modification negatively impacts an individual's ability to perform the generic primary task.

  Examples of negative impacts on an individual's performance that may result in adverse effects on a design function include, but are not limited to:

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

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

SIMPLE HUMAN-SYSTEM INTERFACE EXAMPLE

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

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

Proposed Activity Description

Currently, a knob is rotated clock-wise to open a flow control valve in 1% increments and counter clock-wise to close a flow control valve in 1% increments. This knob will be replaced with a touch screen that has two separate arrows, each in its own function block. Using the touch screen, touching the "up" arrow will open the flow control valve in 1% increments and touching the "down" arrow will close the flow control valve in 1% increments.

HSI Assessment Process

STEP 1. Identification of the Generic Primary Tasks Involved:

(1) Monitoring and detection (extracting information from the

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

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

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

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

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

Identification and Assessment of the Relevant Design Function(s)

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

Using the results from the HFE evaluation and examining the replacement of the "knob" with a "touch screen," the modification is *not adverse* because it does not impact the ability of the operator to "open and close the flow control valve using manual controls located in the Main Control Room," maintaining satisfaction of the UFSAR-described design function.

COMPREHENSIVE HUMAN-SYSTEM INTERFACE EXAMPLES

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

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

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

Proposed Activity Description

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

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

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

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

HSI Assessment Process

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

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

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

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

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

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

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

Identification and Assessment of Design Functions

Design Function Identification

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

(b) The operator controls the system components manually.

Screen Response

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

Although the modification increases the difficulty and amount of time needed for an operator to manipulate a control, the operator is still able to perform design function (b) to manipulate the control for the systems components. Therefore, there is *no adverse* impact on satisfaction of design function (b).

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

Proposed Activity Description

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

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

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

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

HSI Assessment Process

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

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

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

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

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

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

Identification and Assessment of Design Functions

Design Function Identification

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

(b) The operator controls the system components manually.

Screen Response

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

Although the modification increases the difficulty and amount of time needed for an operator to manipulate a control, the operator is still able to perform design function (b) to manipulate the control for the systems components. Therefore, there is *no adverse* impact on satisfaction of design function (b).

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

4.2.1.3 Screening Changes to UFSAR Methods of Evaluation

By definition, a proposed activity involving a digital modification involves SSCs and how SSCs are operated and controlled, not a *method of evaluation* described in the UFSAR (see NEI 96-07, Section 3.10).

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

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

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

By definition, a proposed activity involving a digital modification involves SSCs and how SSCs are operated and controlled, not a test or experiment (see NEI 96-07, Section 4.2.2). The response to this Screen consideration should reflect this characterization.

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

4.3 Evaluation Process

CAUTION

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

Introduction

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

Guidance Focus

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

Example Focus

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

Qualitative Assessment

For digital I&C systems, reasonable assurance of low likelihood of failure is derived from a qualitative assessment of factors involving system design features, the quality of the design processes employed, and the operating history of the software and hardware used (i.e., product maturity and in-service experience). The qualitative assessment is used to record the factors and rationale and reasoning for making a determination that there is reasonable assurance that the digital I&C modification will exhibit a low likelihood of failure by considering the aggregate of these factors.

Software Common Cause Failure Likelihood Determination Outcomes

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

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

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

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

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

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

INTRODUCTION

From NEI 96-07, Section 3.2:

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

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

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

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

For a digital modification, the range of possible equipment-related sources of accident initiators includes items unique to digital and items not unique to digital. An example of an item unique to digital is consideration of the impact on accident frequency due to a software CCF, which will be addressed in this section's guidance. An example of a potential source of common cause failure that is not unique to digital is consideration of the impact on accident frequency due to the digital system's compatibility with the environment in which the system is being installed, which would be addressed by applying the general guidance related to meeting applicable regulatory requirements and other acceptance criteria to which the licensee is committed, and departures from standards as outlined in the general design criteria, as discussed in NEI 96-07, Section 4.3.1 and Section 4.3.1, Example 2.

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

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

GUIDANCE

Determination of Attributable (i.e., Causality)

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

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

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

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

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

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

Proposed Activity Description

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

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

Affected Accidents and Accident Initiators

The review of the UFSAR accident analyses identified the Loss of Coolant Accident (LOCA) and Main Steam Line Break (MSLB) events as containing requirements related to the safety-related containment chillers. Specifically, the UFSAR states the following: "To satisfy single failure requirements, the

loss of only one control system and its worst-case effect on the containment post-accident [emphasis added] environment due to the loss of one chiller has been considered in the LOCA and MSLB analyses."

Therefore, the affected accidents are LOCA and MSLB.

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

Impact on Accident Frequency

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

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

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

Proposed Activity Description

Two non-safety-related main feedwater pumps (MFWPs) exist, each with its own flow control valve. There are two analog control systems (one per MFWP and flow control valve combination) that are physically and functionally the same.

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

Affected Accident and Accident Initiators

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

Impact on Accident Frequency

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

would be assessed next.)

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

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

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

To determine the overall effect of the digital modification on the frequency of an accident, a qualitative assessment of each factor associated with the digital modification and their interdependent relationship need to be considered and addressed as part of the response to this Evaluation criterion, as identified below:

- Software CCF likelihood
- System design features
- Quality of the design processes employed, and
- Operating history of the software and hardware used (i.e., product maturity and in-service experience).

Negligible:

To achieve a *negligible* conclusion, the engineering evaluation (e.g., qualitative assessment) of each factor would conclude that the change in the accident frequency "*...is so small or the uncertainties in determining whether a change in frequency has occurred are such that it cannot be reasonably concluded that the frequency has actually changed (i.e., there is* ***no clear trend toward increasing the frequency)***"[1] [***emphasis*** added] **AND** the software CCF likelihood is **sufficiently low**.

Discernable:

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

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

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

satisfy all applicable NRC requirements, as well as design, material, and construction standards, to which the licensee is committed. Applicable requirements and standards include those selected by the licensee for use in the development of the proposed digital modification and documented within the design modification package.

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

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

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

Proposed Activity Description

Two non-safety-related main feedwater pumps (MFWPs) exist, each with its own flow control valve. There are two analog control systems (one per MFWP and flow control valve combination) that are physically and functionally the same.

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

Magnitude Conclusion

Factors Considered:

- Software CCF likelihood is **sufficiently low**
- System design features
  - Design Criteria - Independence and redundancy are maintained
  - Inherent Design Features for Software, Hardware or the Architectural/Network - Watchdog timers that operate independently of software, isolation devices, segmentation, self-testing and self-diagnostic features exist
  - Non-concurrent Triggers - Verified
  - Software Architecture Complexity - Tested to the extent possible
  - Unlikely Series of Events - Multiple independent random failures are not possible
  - Failure State - All states are known to be acceptable
- Quality of the design processes employed - The control system equipment vendor employed quality standards commensurate with the importance of

the functions to be performed.
- Operating history of the software and hardware used (i.e., product maturity and in-service experience) - A review of the available operating history of the hardware and software was performed and documented. No examples of unexplained failures or behaviors were identified.

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

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

Overall Conclusion

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

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

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

Proposed Activity Description

Same as Example 4-11.

Magnitude Conclusion

Factors Considered:

Based on an engineering evaluation performed as part of the technical assessment supporting this digital modification, the likelihood of a software CCF causing the loss of both feedwater control systems (resulting in the loss of both MWFPs) has been determined to be **not sufficiently low**.

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

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

Overall Conclusion

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

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

HUMAN-SYSTEM INTERFACE ASSESSMENT

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

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

INTRODUCTION

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

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

For a digital modification, the range of possible equipment-related sources of malfunction initiators includes items unique to digital and items not unique to digital. An example of an item unique to digital is consideration of the impact on malfunction likelihood due to a software CCF, which will be

addressed in this section's guidance. An example of a potential source of common cause failure that is not unique to digital is consideration of the impact on malfunction likelihood due to the digital system's compatibility with the environment in which the system is being installed, which would be addressed by applying the general guidance related to meeting applicable regulatory requirements and other acceptance criteria to which the licensee is committed, and departures from standards as outlined in the general design criteria, as discussed in NEI 96-07, Section 4.3.2.

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

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

GUIDANCE

Impact on Redundancy, Diversity, Separation or Independence

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

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

Redundancy:

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

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

Diversity:

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

> "*Criterion 22 -- Protection system independence. The protection system shall be designed to assure that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection*

function, or shall be demonstrated to be acceptable on some other defined basis. ***Design techniques, such as functional diversity or diversity in component design and principles of operation****, shall be used to the extent practical to prevent loss of the protection function.*" [***emphasis*** added]

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

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

Separation:

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

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

Independence:

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

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

Determination of Attributable (i.e., Causality)

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

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

Alternately, if any components/systems involved with the digital modification are identified as affecting a malfunction initiator previously identified in the

UFSAR, then an impact on the likelihood of occurrence of a malfunction can be attributed to the digital modification. If an attributable impact is identified, then further assessment to determine the magnitude of the impact will be performed.

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

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

Proposed Activity Description

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

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

Affected Malfunctions and Malfunction Initiators

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

Impact on Malfunction Likelihood

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

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

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

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

To determine the overall effect of the digital modification on the likelihood of a malfunction, a qualitative assessment of each factor associated with the digital modification and their interdependent relationship need to be considered and addressed as part of the response to this Evaluation criterion, as identified below:

- Software CCF likelihood
- System design features
- Quality of the design processes employed, and
- Operating history of the software and hardware used (i.e., product maturity and in-service experience).

Negligible:

To achieve a *negligible* conclusion, the engineering evaluation (e.g., qualitative assessment) of each factor would conclude that the change in the malfunction likelihood "*...is so small or the uncertainties in determining whether a change in likelihood has occurred are such that it cannot be reasonably concluded that the likelihood has actually changed (i.e., there is* ***no clear trend toward increasing the likelihood)***"[2] [***emphasis*** added] **AND** the software CCF likelihood is **sufficiently low**.

Discernable:

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

The engineering evaluation (e.g., qualitative assessment) is also used to determine if the discernible increase in the malfunction likelihood is "more than minimal" or "NOT more than minimal." To achieve a conclusion of "NOT more than minimal," the proposed activity must continue to meet and/or satisfy all applicable NRC requirements, as well as design, material, and construction standards, to which the licensee is committed. Applicable requirements and standards include those selected by the licensee for use in

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

the development of the proposed digital I&C design modification and documented within the design modification package.

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

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

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

Proposed Activity Description

Two non-safety-related main feedwater pumps (MFWPs) exist, each with its own flow control valve. There are two analog control systems (one per MFWP and flow control valve combination) that are physically and functionally the same.

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

Magnitude Conclusion

Factors Considered:

- Software CCF likelihood is **sufficiently low**
- System design features
  - Design Criteria - Independence and redundancy are maintained
  - Inherent Design Features for Software, Hardware or the Architectural/Network - Watchdog timers that operate independently of software, isolation devices, segmentation, self-testing and self-diagnostic features exist
  - Non-concurrent Triggers - Verified
  - Software Architecture Complexity - Tested to the extent possible
  - Unlikely Series of Events - Multiple independent random failures are not possible
  - Failure State - All states are known to be acceptable
- Quality of the design processes employed - The control system equipment vendor employed quality standards commensurate with the importance of the functions to be performed.
- Operating history of the software and hardware used (i.e., product maturity and in-service experience) - A review of the available operating

---

history of the hardware and software was performed and documented. No examples of unexplained failures or behaviors were identified.

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

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

Overall Conclusion

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

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

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

Proposed Activity Description

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

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

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

Affected Malfunction and Malfunction Initiator

The review of the UFSAR accident analyses identified several events for which the safety injection pumps are assumed to start and operate (as

reflected in the inputs and assumptions to the accident analyses).

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

Magnitude Conclusion

Factors Considered:

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

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

Overall Conclusion

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

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

HUMAN-SYSTEM INTERFACE ASSESSMENT

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

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

There is no unique guidance applicable to digital modifications for responding to this Evaluation criterion because the identification of affected accidents and dose analysis inputs and/or assumptions are not unique for a digital modification. The guidance in NEI 96-07, Section 4.3.3 applies.

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

There is no unique guidance applicable to digital modifications for responding to this Evaluation criterion because the identification of the affected malfunctions and dose analysis inputs and/or assumptions are not unique for a digital modification. The guidance in NEI 96-07, Section 4.3.4 applies.

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

INTRODUCTION

From NEI 96-07, Section 3.2:

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

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

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

GUIDANCE

Determination of Credible

From NEI 96-07, Section 4.3.5:

> "*The possible accidents of a different type are limited to those that are as likely to happen as those previously evaluated in the UFSAR. The accident must be credible in the sense of having been created within the range of assumptions previously considered in the licensing basis (e.g., random single failure, loss of off-site power, etc.).*"

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

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

If the software CCF likelihood is determined to be **not sufficiently low**, then the creation of a possibility for an accident of a different type is *credible*. If the creation of a possibility for an accident of a different type is credible, then further assessment to determine the accident analysis impact will be performed.

Determination of Accident Analysis Impact

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

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

There are two possible impacts on the accident analysis:

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

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

Accidents of a different type are credible accidents for which a new accident analysis would be needed, not just a revision of a current accident analysis.

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

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

Proposed Activity

Two non-safety-related main feedwater pumps (MFWPs) exist, each with its own flow control valve. There are two analog control systems (one per MFWP and flow control valve combination) that are physically and functionally the same.

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

Malfunction / Accident Initiator

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

system.

Accident Frequency and Type

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

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

Accident Category - Infrequent Incident

Credible Conclusion

Based on an engineering evaluation performed as part of the technical assessment supporting this digital modification, the likelihood of a software CCF causing the loss of both feedwater control systems (resulting in the loss of both MWFPs) has been determined to be **sufficiently low**.

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

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

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

Proposed Activity

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

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

Malfunction / Accident Initiator

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

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

Accident Frequency and Type

The characteristics of the pertinent accidents are as follows:

Loss of Feedwater:

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

Accident Category - Infrequent Incident

Excess Feedwater:

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

Accident Category - Moderate Frequency Incident

Loss of Load:

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

Accident Category - Moderate Frequency Incident

Excess Steam Demand:

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

Accident Category - Moderate Frequency Incident

Credible Conclusion

Based on an engineering evaluation performed as part of the technical assessment supporting this digital modification, the likelihood of a software CCF impacting both the feedwater control systems and the main turbine steam-inlet valves control system has been determined to be **not sufficiently low**.

Therefore, in this case, the following conditions are *credible* creating a possibility for several accidents:

(1) Loss of both feedwater pumps

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

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

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

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

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

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

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

Accident Analysis Impact Conclusion

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

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

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

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

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

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

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

HUMAN-SYSTEM INTERFACE ASSESSMENT

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

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

[LATER]

HUMAN-SYSTEM INTERFACE ASSESSMENT

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

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

There is no unique guidance applicable to digital modifications for responding to this Evaluation question because the identification of possible design basis limits for fission product barriers and the process for determination of "exceeded" or "altered" are not unique for a digital modification. The guidance in NEI 96-07, Section 4.3.7 applies.

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

There is no unique guidance applicable to digital modifications for responding to this Evaluation criterion because activities involving *methods of evaluation* do not involve SSCs. The guidance in NEI 96-07, Section 4.3.8 applies.

5.0 EXAMPLES

[LATER]