NEI TECHNICAL REPORT

NEI 96-07
Appendix D, Rev 1

SUPPLEMENTAL GUIDANCE FOR APPLICATION OF 10 CFR 50.59 TO DIGITAL MODIFICATIONS

Prepared by the Nuclear Energy Institute
~~November 2018~~February 2020

Acknowledgements

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.

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*, and incorporates the 10 CFR 50.59-related guidance contained in Regulatory Issue Summary (RIS) 2002-22, Supplement 1, *Clarification on Endorsement of Nuclear Energy Institute Guidance in Designing Digital Upgrades in Instrumentation and Control Systems*.

Table of Contents

1 INTRODUCTION

There are specific considerations that should be addressed as part of the 10 CFR 50.59 process when performing 10 CFR 50.59 reviews for digital modifications. These specific considerations include different potential failure modes of digital equipment as opposed to the equipment being replaced, the effect of combining functions of previously separate devices (at the component level, at the system level, or at the "multi-system" level) into fewer devices or one device, and the potential for software common cause failure (software CCF).

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

1.1 Background

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. Also, there is great incentive to take advantage of modern digital technologies that 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 concerns 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 "mixture of guidance" as an issue and stated that NEI should separate the technical guidance from the 10 CFR 50.59 guidance.

In 2018, Supplement 1 to RIS 2002-22 was issued to clarify the NRC staff's endorsement of the guidance pertaining to NEI 01-01, Sections 4 and 5 and Appendices A and B. Specifically, the RIS supplement clarified the guidance for preparing and documenting "qualitative assessments" that may be used to evaluate the likelihood of failure of a proposed digital modification, including the likelihood of failure due to a software common cause failure (software CCF).

Supplement 1 to RIS 2002-22 identified that a qualitative assessment may be used to support a conclusion that a proposed digital I&C modification will not result in more than a minimal increase in the frequency of occurrence of accidents or in the likelihood of occurrence of malfunctions (10 CFR 50.59(c)(2)(i) and (ii)). A qualitative assessment may also be used to support a conclusion that the proposed modification does not create the possibility of an accident of a different type or a malfunction

with a different result than previously evaluated in the updated final safety analysis report (10 CFR 50.59(c)(2)(v) and (vi)).

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. Appendix D does not alter and, unless explicitly noted, should not be interpreted differently than the guidance contained in NEI 96-07, Rev. 1. Rather, Appendix D provides focused guidance for the application of 10 CFR 50.59 to activities involving digital modifications.

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 involve 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

Relationship of Appendix D to NEI 96-07, Revision 1

In sections 3 and 4 of this appendix, references to the main body of NEI 96-07, Revision 1 will be abbreviated as "NEI 96-07."

Guidance Focus

In Sections 4.2 (Screening) and 4.3 (Evaluation), each section and sub-section addresses only a specific aspect, sometimes at the ***deliberate exclusion of other pertinent and/or related aspects***.

This focused approach is intended to concentrate the guidance 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

Unless stated otherwise, a given example addresses ONLY the aspect within the section/sub-section in which it is included, sometimes at the ***deliberate exclusion of other pertinent and/or related aspects*** which, if considered, could potentially change the Screen and/or Evaluation conclusion(s).

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.

Definitions specific to this appendix are defined below.

3.15 Qualitative Assessment

Definition:

A **qualitative assessment** is a specific type of technical-based engineering evaluation useful to 10 CFR 50.59 Evaluations when responding to Evaluation criteria 10 CFR 50.59(c)(2(i), (ii), (v) and (vi).

Discussion:

The purpose of a **qualitative assessment** is to determine the "magnitude" of the likelihood of a software CCF. The magnitude of the likelihood of a software CCF can be either *sufficiently low* (see the definition in Section 3.16) or *not sufficiently low*. Therefore, the only part of the **qualitative assessment** needed for responding to the four 10 CFR 50.59(c)(2) criteria listed above is the outcome (i.e., *sufficiently low* or *not sufficiently low*).

Although a **qualitative assessment** could be performed as part of developing the responses to the four 10 CFR 50.59(c)(2) criteria listed above, this technical-based engineering evaluation is typically performed "prior to" or "in parallel with" the completion of the 10 CFR 50.59 Evaluation.

Generally, reasonable assurance of the low likelihood of failure due to a software CCF is derived from the **qualitative assessment** of factors involving (1) the design attributes of the modified SSC, (2) the quality of the design processes, and (3) the operating experience of the software and hardware used (i.e., product maturity and in-service experience).

The **qualitative assessment** is used to record the factors and rationale for making a determination of the likelihood of failure (i.e., *sufficiently low* or *not sufficiently low*) due to a software CCF that a digital I&C modification will exhibit.

The determination of the likelihood of failure may consider the aggregate of all the factors described above. Namely, some of the factors may compensate for weaknesses in other areas or other factors. For example, thorough testing coupled with an analysis demonstrating untested states are accounted for in the proposed application may provide additional assurance of a *sufficiently low* likelihood of failure to compensate for a lack of operating experience.

A **qualitative assessment** should not be used for digital I&C replacements of the reactor protection system (RPS), the engineered safety features actuation system (ESFAS), or modification/replacement of the internal logic portions of these systems (e.g., voting logic, bistable inputs, and signal conditioning/processing).

3.16 Sufficiently Low

Definition:

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).

Discussion:

This **sufficiently low** threshold is not interchangeable with that used for distinguishing between events that are "credible" or "not credible." The threshold for determining if an event is credible uses the criterion of "as likely as" (i.e., not "much lower than") the malfunctions already assumed in the UFSAR.

4 IMPLEMENTATION GUIDANCE

4.1 Applicability

No additional guidance is provided.

4.2 Screening

CAUTION

The guidance contained in this section of the 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

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 times, 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.

Human-System Interface Considerations

Similar to other technical evaluations (performed as part of the design modification package), a human factors engineering (HFE) evaluation determines the impacts and outcomes of the change (e.g., personnel acts or omissions, as well as their likelihoods and effects). The licensing-based reviews (Screens and Evaluations) performed in accordance with 10 CFR 50.59 compare the impacts and new outcomes (i.e., post-modification) to the initial conditions and current outcomes (i.e., pre-modification) in order to determine the effect on design functions (in the Screen phase) and the need for a license amendment request (in the Evaluation phase).

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

Introduction

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.) with a touch-screen to operate or control plant equipment.

Engineering/technical information should be documented (as part of the design process) to record the impacts from digital modifications. This engineering/technical information will be used as the basis/justification for the conclusion of *adverse* or *not adverse*.

Scope of Digital Modifications

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

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

Based on this segmentation of activities, the software and hardware portions will be assessed within the "facility" Screen consideration since these aspects involve SSCs, SSC design functions, or the method of performing or controlling a design function and the Human-System Interface (HSI) 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

Discussion

For applications involving SSCs with design functions, an adverse effect may be created due to the potential marginal increase in the likelihood of SSC failure due to the introduction of software. This does not mean that all digital modifications that introduce software will automatically screen-in.

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, the engineering/technical information supporting the change may show that the digital modification contains design attributes to eliminate consideration of a software common cause failure. In such cases, even when a digital modification involves redundant systems, the digital modification would not be adverse.

For relatively simple digital modifications, engineering/technical information supporting the change may be used to show that the digital modification would not adversely affect design functions; even for digital modifications that involve redundant components/systems because a software CCF is *not introduced*.

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

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

EXAMPLES

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 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.

Failures of the new digital device are encompassed by the failures of the existing analog device. The engineering/technical information supporting the change concluded that the digital system is at least as reliable as the previous system, the conclusion of which is based on the quality of the design processes employed, and the operating history of the software and hardware used. In addition, based on the simplicity of the device, 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* (for the aspect being illustrated in this example) 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 a software CCF is not introduced.

Example 4-2 illustrates the application of the Use of Software and Digital Devices aspect.

Example 4-2. 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.

No combination of components/systems and/or functions occurs as part of this digital modification.

Design Function Identification

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

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 (for the aspect being illustrated in this example) 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 potential software CCF that did not previously exist.

COMBINATION OF COMPONENTS/SYSTEMS AND/OR FUNCTIONS

Discussion

The UFSAR may identify the number of components/systems, how the components/systems are arranged and/or how functions are 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 *design functions*.

The mere act of combining previously separate components/systems and/or functions does not make the Screen conclusion adverse. However, if combining the previously separate components/systems and/or functions causes an adverse impact on a *design function* (e.g., by causing the loss of multiple design functions when the digital device fails), then the combination aspect of the digital modification will have an adverse impact on a *design function* (i.e., 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*.

Furthermore, digital modifications that involve networking; combining design functions from different systems; interconnectivity across channels, systems, and divisions; or shared resources, merit careful review to determine if such modifications cause reductions in the redundancy, diversity, separation, or independence of UFSAR-described design functions.

Combining different functions due to digital modifications can result in combining design functions of different systems; either directly in the same digital device, or indirectly through shared resources. Shared resources (e.g., bidirectional communications, power supplies, controllers, and multifunction display and control stations) introduced by digital modifications may reduce the redundancy, diversity, separation, or independence of UFSAR-described design functions.

Reductions in the redundancy, diversity, separation, or independence of a UFSAR-described design function have an adverse impact on that design function.

EXAMPLES

Examples 4-3 through 4-5 illustrate the application of *the Combination of Components/Systems and/or Functions* aspect.

Example 4-3. Combining Components and Functions with NO ADVERSE IMPACT (Option #1) and an ADVERSE IMPACT (Option #2) 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 and sub-components in each analog control system will be replaced with their own digital control system, retaining two discreet, unconnected control systems.

Option #2: Instead of two discreet, unconnected digital control systems being used for the feedwater control systems (as outlined in Option #1), only **one** digital device is proposed to be used that will combine ALL components, sub-components and functions of both control systems.

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.

Screen Response

Option #1: There is *no adverse* impact (for the aspect being illustrated in this example) 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 two feedwater control systems are maintained.

Option #2: There is an *adverse* impact (for the aspect being illustrated in this example) 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 loss of the one digital device would cause multiple design functions (one each from the two original feedwater control systems) to NOT be performed.

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

Proposed Activity Description

A temperature monitor/controller in a room containing an emergency room cooler 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 control the temperature in the room by continuously monitoring the temperature in the room to ensure the initial conditions are met should the emergency room cooler be needed.

The air damper controller performs a design function to control the temperature in the room by continuously providing the appropriate air flow to the room to ensure the initial conditions are met should the emergency room cooler be needed.

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

Screen Response

In the current design, a failure of the temperature monitor/controller or the air damper controller causes the loss of the ability to control the temperature in the room. In the proposed design, the failure of the digital device causes multiple failures, but still only the loss of the ability to control the temperature in the room. With the loss of ability to control temperature in the room being the same in the current design and in the proposed design, there is no adverse impact (for the aspect being illustrated in this example) on the design function.

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

Example 4-5 illustrates the combining of control systems from different, originally discrete systems.

Example 4-5. Combining Systems and Functions with an ADVERSE IMPACT on a Design Function

Proposed Activity Description

One non-safety-related analog Steam Bypass Control System (SBCS) and one non-safety-related main turbine steam inlet valves analog control system exist.

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

Design Function Identification

The design function of the SBCS is to maximize plant availability by making full utilization of the turbine bypass valve capacity to remove Nuclear Steam Supply System (NSSS) thermal energy to accommodate load rejections, unit trips, and other conditions that result in the generation of excessive energy by the NSSS. This objective is achieved by the selective use of turbine bypass valves to avoid unnecessary reactor trips and prevent the opening of secondary side safety valves whenever these occurrences can be averted by the controlled release of steam.

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

Screen Response

Because the failure of the new, single digital device will cause the loss of multiple design functions, the digital modification has an *adverse* impact (for the aspect being illustrated in this example) on the design function of the SBCS and the design function of the main turbine steam inlet valves control system.

4.2.1.2 Screening of Changes to Procedures as Described in the UFSAR

SCOPE

If the digital modification does not include or affect an HSI element (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 HSI, UFSARs may describe 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.

HUMAN FACTORS ENGINEERING (HFE) EVALUATION

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.

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)

Table 1 - Example Human-System Interface Modifications

To determine potential adverse impacts of HSI modifications on design functions, a two-step HFE evaluation 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 impacts on an individual's performance that 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.

GUIDANCE

After the two-step HFE evaluation, the next step is application of the standard Screen process.

Simple Human-System Interface Example

Example 4-6 illustrates how a digital modification with HSI considerations would be addressed.

Example 4-6: 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.

HFE Evaluation

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:

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

Task 4 is involved. The HFE evaluation determined that the change from knob to touch screen would not impact the operator's ability to perform the response implementation task.

Identification and Assessment of Design Functions

Design Function Identification

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

Screen Response

Using the results from the engineering/technical information supporting the change, including the HFE evaluation, and examining the replacement of the "knob" with a "touch screen," the modification is *not adverse* (for the aspect being illustrated in this example) 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 how the UFSAR-described design function is performed or controlled.

Comprehensive Human-System Interface Examples

Examples 4-7 and 4-8 illustrate how a digital modification with HSI considerations would be addressed.

Although both examples use the same basic digital modification, Example 4-7 illustrates a no adverse impact case and Example 4-8 illustrates an adverse impact case by complicating the HSI portion of the modification and modifying the applicable licensing basis.

Example 4-7. 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.

HFE Evaluation

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) – NOTINVOLVED
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:

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~~ appropriatly sized flat panels, appropriate display brightness, clearly identified function buttons, etc.), as documented in the HFE evaluation, there is no impact on 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 impacts the operator's ability to respond by requiring four actions instead of one action and the additional actions result in an increase in the operator's time to respond. However, the HFE evaluation concluded that the operator actions continue to take place and can be performed in a timely and comparable manner.

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.

In this case, the review of the UFSAR, including the assumptions described in the safety analyses, determined that there were no additional design functions related to how design function (b) was performed or controlled. Namely, there were no design functions related to the number of steps necessary to perform the design function (i.e., complexity) or the duration in which the steps were to be performed (i.e., time response).

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 (for the aspect being illustrated in this example) on design function (a).

Using the touch screen, the operator is still able to perform design function (b) to manipulate the control for the systems components. Therefore, there is *no adverse* impact (for the aspect being illustrated in this example) on how design function (b) is performed or controlled because the HFE evaluation concluded that the operator actions continue to take place and could be performed in a timely and comparable manner.

Example 4-8. 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.

HFE Evaluation

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:

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 impacting their ability to monitor the plant and detect changes. In addition, altering the information displayed and the organization of the information will impact the operator's understanding of how the information relates to system performance. This impact on understanding will also 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 impacts the operator's ability to respond by requiring four actions instead of one action and the additional actions result in an increase in the operator's time to respond. However, the HFE evaluation concluded that the operator actions continue to take place and can be performed in a timely and comparable manner.

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.

The review of the UFSAR, including the assumptions described in the safety analysis, determined that an additional design function related to how design function (b) was performed exists. Namely, in the pertinent safety analysis, a response time requirement of the operator had been credited.

Screen Response

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

Using the touch screen, the operator is still able to perform design function (b) to manipulate the

control for the systems components. However, there is *no adverse* impact (for the aspect being illustrated in this example) on how design function (b) is performed due to the increased response time because the HFE evaluation concluded that the operator actions continue to take place and could be performed in a timely and comparable manner.

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

CAUTION

The guidance contained in this section of the 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.

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, the change is examined to determine if the frequency of these accidents could increase due to the change. When addressing this Evaluation criterion for digital upgrades, the key issue is determining if the digital equipment can increase the frequency of initiating events that lead to the identified accidents.

All initiating events 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 initiating events includes items unique to digital and items not unique to digital. An example of an item unique to digital is consideration of the impact on accident frequency due to a software CCF, which will be addressed in this guidance. An example of a potential source of common cause failure that is not unique to digital is consideration of the impact on accident frequency due to the digital system's compatibility with the environment in which the system is being installed, which would be addressed by applying the general guidance in NEI 96-07, Section 4.3.1.

Typically, numerical values quantifying an accident frequency are not available, so the qualitative approach using the guidance from NEI 96-07, Section 4.3.1 will be applied in this guidance.

The frequency of occurrence of an accident is directly related to the likelihood of failure of equipment that initiates the accident (e.g., an increase in the likelihood of a steam generator tube failure has a

corresponding increase in the frequency of a steam generator tube rupture accident). Thus, an increase in the likelihood of failure of the modified equipment causes an increase in the frequency of the accident.

GUIDANCE

Qualitative Assessment Outcome

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

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

Negligible

To achieve a negligible conclusion, 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]

Discernable

If a clear trend towards increasing the accident frequency exists, then a *discernable* increase in the accident frequency would exist. In this case, the software CCF likelihood would be **not sufficiently low**.

In this case, the engineering/technical information supporting the change (e.g., a *qualitative assessment* and/or any other supporting information) should be used to assess the qualitative increase in the magnitude of the accident frequency and determine if the *discernable* increase in the accident frequency is "more than minimal" or "NOT more than minimal."

As part of the assessment to determine the qualitative increase in the magnitude of the accident frequency, the concept of interdependence also needs to be considered and applied. Namely, interdependence considers the overall impact due to the change. For example, the "negative" impact due to a software CCF likelihood being **not sufficiently low** could be partially or wholly offset by the "positive" impacts due to the digital system/component itself and/or its design features.

Finally, to achieve a conclusion of "NOT more than minimal" based on the engineering/technical information supporting the change, the proposed activity must also continue to meet and/or satisfy all applicable NRC requirements, as well as design, material, and construction standards, to which the licensee is committed. Applicable requirements and standards include those selected by the licensee for use in the development of the proposed digital modification and documented within the design modification package.

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

EXAMPLES

Example 4-9 illustrates a case with not more than a minimal increase in the accident frequency.

Example 4-9. NOT MORE THAN A MINIMAL Increase in 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.

Qualitative Assessment Outcome

A *qualitative assessment* was included in the engineering/technical information supporting the change. The *qualitative assessment* considered system design attributes, quality of the design processes employed, and operating experience of the proposed equipment and concluded that the failure likelihood introduced by the modified SSC is **sufficiently low**. For the specific items that were considered within each factor, refer to the *qualitative assessment* documented in design change package X.

Conclusion

With the failure likelihood introduced by the modified SSC being **sufficiently low**, there is **not** more than a minimal increase in the frequency of occurrence of an accident previously evaluated in the UFSAR (for the aspect being illustrated in this example).

Example 4-10 illustrates a case with more than a minimal increase in the accident frequency.

Example 4-10. MORE THAN A MINIMAL Increase in the Frequency of Occurrence of an Accident

Proposed Activity Description

Same as Example 4-9.

Qualitative Assessment Outcome

A *qualitative assessment* was included in the engineering/technical information supporting the change. The *qualitative assessment* considered system design attributes, quality of the design processes employed, and operating experience of the proposed equipment and concluded that the failure likelihood introduced by the modified SSC is **not sufficiently low**. For the specific items that were considered within each factor, refer to the *qualitative assessment* documented in design change package X.

Conclusion

As documented in the *qualitative assessment*, the features of the design process and operating experience were insufficient to offset weaknesses in the design attributes that were available to prevent

certain failures. For the specific items that were considered within each factor, refer to the *qualitative assessment* documented in design change package X.

With the failure likelihood introduced by the modified SSC being **not sufficiently low** and the inability to offset weaknesses in the design attributes, there is more than a minimal increase in the frequency of occurrence of the accident previously evaluated in the UFSAR (for the aspect being illustrated in this example)~~.~~.

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, the change is examined to determine if the likelihood of these malfunctions could increase due to the change. When addressing this Evaluation criterion for digital upgrades, the key issue is determining if the digital equipment can increase the likelihood of initiating events that lead to the identified malfunctions.

All initiating events 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 initiating events includes items unique to digital and items not unique to digital. An example of an item unique to digital is consideration of the impact on malfunction likelihood due to a software CCF, which will be addressed in this guidance. An example of a potential source of common cause failure that is not unique to digital is consideration of the impact on malfunction likelihood due to the digital system's compatibility with the environment in which the system is being installed, which would be addressed by applying the general guidance in NEI 96-07, Section 4.3.2.

Typically, numerical values quantifying a malfunction likelihood are not available, so the qualitative approach using the guidance from NEI 96-07, Section 4.3.2 will be applied in this guidance.

The likelihood of occurrence of a malfunction of an SSC important to safety is directly related to the likelihood of failure of equipment that causes a failure of SSCs to perform their intended design functions [e.g., an increase in the likelihood of failure of an auxiliary feedwater (AFW) pump has a corresponding increase in the likelihood of occurrence of a malfunction of SSCs (i.e., the AFW pump and the AFW system)]. Thus, an increase in the likelihood of failure of the modified equipment that causes the failure of an SSC to perform its intended design functions is directly related to the likelihood of the occurrence of a malfunction of an SSC important to safety.

Digital modifications that involve networking; combining design functions from different systems; interconnectivity across channels, systems, and divisions; or shared resources, merit careful review to determine if such modifications cause reductions in the redundancy, diversity, separation, or independence of UFSAR-described design functions.

Combining different functions due to digital modifications can result in combining design functions of different systems; either directly in the same digital device, or indirectly through shared resources. Shared resources (e.g., bidirectional communications, power supplies, controllers, and multifunction display and control stations) introduced by digital modifications may reduce the redundancy, diversity, separation, or independence of UFSAR-described design functions.

GUIDANCE

As discussed in NEI 96-07, Section 4.3.2, Example 6, a proposed activity that reduces redundancy, diversity, separation or independence of the design function(s) 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 UFSAR without prior NRC approval.

The possibility exists that a proposed activity can cause a previously incredible event to become credible.

Example 4-11 illustrates a case in which a previously incredible event has become credible due to a digital modification.

Example 4-11. 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 Initiating Events

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 initiating events 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 initiating events 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 initiating event 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 due to the digital modification has occurred. (NOTE: The magnitude of the impact would then need to be assessed using the engineering/technical information supporting the change and the

concepts of interdependence described in NEI 96-07, Section 4.3.)

Qualitative Assessment Outcome

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

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

Negligible

To achieve a *negligible* conclusion, 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 qualitative assessment outcome for a software CCF will be **sufficiently low**.

Discernable

If a clear trend towards increasing the malfunction likelihood exists, then a *discernable* increase in the malfunction likelihood would exist. In this case, the software CCF likelihood would be **not sufficiently low.**

In this case, the engineering/technical information supporting the change (e.g., a *qualitative assessment* and/or any other supporting information) should be used to assess the qualitative increase in the magnitude of the malfunction likelihood and determine if the *discernable* increase in the malfunction likelihood is "more than minimal" or "NOT more than minimal."

As part of the assessment to determine the qualitative increase in the magnitude of the malfunction likelihood, the concept of interdependence also needs to be considered and applied. Namely, interdependence considers the overall impact due to the change. For example, the "negative" impact due to a software CCF likelihood being **not sufficiently low** could be partially or wholly offset by the "positive" impacts due to the digital system/component itself and/or its design features.

Finally, to achieve a conclusion of "NOT more than minimal" based on the engineering/technical information supporting the change, the proposed activity must also continue to meet and/or satisfy all applicable NRC requirements, as well as design, material, and construction standards, to which the licensee is committed. Applicable requirements and standards include those selected by the licensee for use in the development of the proposed digital I&C design modification and documented within the design modification package.

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

EXAMPLES

Example 4-12 illustrates a case with not more than a minimal increase in the malfunction likelihood.

Example 4-12. NOT MORE THAN A MINIMAL Increase 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.

Qualitative Assessment Outcome

A *qualitative assessment* was included in the engineering/technical information supporting the change. The *qualitative assessment* considered system design attributes, quality of the design processes employed, and operating experience of the proposed equipment and concluded that the failure likelihood introduced by the modified SSC is **sufficiently low**. For the specific items that were considered within each factor, refer to the *qualitative assessment* documented in design change package X.

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.

Conclusion

With the failure likelihood introduced by the modified SSC being **sufficiently low**, there is **not** more than a minimal increase in the likelihood of occurrence of a malfunction of an SSC important to safety previously evaluated in the UFSAR (for the aspect being illustrated in this example).

Example 4-13 illustrates a case with more than a minimal increase in the malfunction likelihood.

Example 4-13. MORE THAN A MINIMAL 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

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 for 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 analysis."

Qualitative Assessment Outcome

A *qualitative assessment* was included in the engineering/technical information supporting the change. The *qualitative assessment* considered system design attributes, quality of the design processes employed, and operating experience of the proposed equipment and concluded that the failure likelihood introduced by the modified SSC is **not sufficiently low**. For the specific items that were considered within each factor, refer to the *qualitative assessment* documented in design change package X.

An increase in the likelihood of occurrence of the malfunction of both safety injection pumps occurs since the single failure criteria are no longer met.

Conclusion

With the failure to satisfy single failure criteria, there is more than a minimal increase in the likelihood of occurrence of the malfunction of the safety injection pumps due to the digital modification. As documented in the *qualitative assessment*, the features of the design process and operating experience were insufficient to offset weaknesses in the design attributes that were available to prevent certain failures. For the specific items that were considered within each factor, refer to the *qualitative assessment* documented in design change package X.

With the failure likelihood introduced by the modified SSC being **not sufficiently low** and the inability to offset weaknesses in the design attributes, there is more than a minimal increase in the likelihood of occurrence of a malfunction previously evaluated in the UFSAR (for the aspect being illustrated in this example).

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."

GUIDANCE

From NEI 96-07, Section 4.3.5, the two considerations that need to be assessed when answering this Evaluation question are *as likely to happen as* and *accident of a different type*.

Determination of "As Likely To Happen As"

From NEI 96-07, Section 4.3.5:

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

If the outcome of the *qualitative assessment* is **sufficiently low**, then the activity does not introduce any failures that are as likely to happen as those in the UFSAR that can initiate an accident of a different type. Therefore, the activity does not create a possibility for an accident of a different type than any previously evaluated in the UFSAR.

If the outcome of the *qualitative assessment* is **not sufficiently low**, then the activity may introduce failures that are as likely to happen as those in the UFSAR that can initiate an accident of a different type, i.e., the activity created a possibility. For these cases, this Evaluation criterion also needs to consider an accident of a different type.

Determination of "Accident of a Different Type"

For cases in which the outcome of the *qualitative assessment* is **not sufficiently low**, an *accident of a different type* needs to be determined, as follows:

If a **revision** to an existing accident analysis is to be performed, then the proposed activity does NOT create the possibility of an accident of a different type.

If a **new** accident analysis is needed, then the proposed activity DOES create the possibility of an accident of a different type.

EXAMPLES

Example 4-14 illustrates the NO CREATION of the possibility of an accident of a different type case.

Example 4-14. 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.

Qualitative Assessment Outcome

A *qualitative assessment* was included in the engineering/technical information supporting the change. The *qualitative assessment* considered system design attributes, quality of the design processes employed, and operating experience of the proposed equipment and concluded that the failure likelihood introduced by the modified SSC is **sufficiently low**. For the specific items that were considered within each factor, refer to the *qualitative assessment* documented in design change package X.

Conclusion

With the failure likelihood introduced by the modified SSC being **sufficiently low**, the activity does not introduce any failures that are as likely to happen as those in the UFSAR that can initiate an accident of a different type. Therefore, the activity does not create a possibility for an accident of a different type than any previously evaluated in the UFSAR (for the aspect being illustrated in this example).

Example 4-15 illustrates the CREATION of the possibility of an accident of a different type case.

Example 4-15. 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.

Qualitative Assessment Outcome

A *qualitative assessment* was included in the engineering/technical information supporting the change. The *qualitative assessment* considered system design attributes, quality of the design processes employed, and operating experience of the proposed equipment and concluded that the failure likelihood introduced by the modified SSC is **not sufficiently low**. For the specific items that were considered within each factor, refer to the *qualitative assessment* documented in design change package X.

Malfunction / Accident Identification

The UFSAR describes the following feedwater control system malfunctions: (a) failures causing the loss of all feedwater to the steam generators, which is evaluated in the Loss of Feedwater event, and (b) failures causing an increase in main feedwater flow to the maximum output from both MFWPs, which is evaluated in the Excess Feedwater event.

The UFSAR describes the following main turbine steam-inlet valves control system malfunctions: (a) all valves going fully closed causing no steam to be admitted into the turbine, which is evaluated in the Turbine Trip event, and (b) all valves going fully open causing excess steam to be admitted into the turbine, which is evaluated in the Excess Steam Demand event.

Therefore, the impact of the failures that are as likely to happen as those in the UFSAR that can initiate an accident of a different type will be assessed for the following accident analyses:

1. Loss of Feedwater
2. Excess Feedwater
3. Turbine Trip
4. Excess Steam Demand

Accident of a Different Type Assessment

The following events and combination of events will be assessed:

a. Loss of both feedwater pumps in the Loss of Feedwater accident analysis
b. Increase in main feedwater flow to the maximum output from both MFWPs in the Excess Feedwater accident analysis
c. All main turbine steam-inlet valves going fully closed in the Turbine Trip accident analysis
d. All main turbine steam-inlet valves going fully open in the Excess Steam Demand accident analysis
e. Combination of a Loss of Feedwater event and a Turbine Trip event
f. Combination of a Loss of Feedwater event and an Excess Steam Demand event
g. Combination of an Excess Feedwater event and a Turbine Trip event
h. Combination of an Excess Feedwater event and an Excess Steam Demand event

Events (A) though (D) are already considered in the accident analyses and revisions to existing accident analyses are possible. Thus, events (A) through (D) do NOT create the possibility of an accident of a different type (for the aspect being illustrated in this example).

The current set of accidents identified in the accident analyses do not consider the simultaneous events represented by events (E) through (H).

Therefore, events (E) though (H) will need new accident analyses to be performed, creating the possibility of accidents of a different type (for the aspect being illustrated in this example).

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

INTRODUCTION

NOTE: Due to the unique nature of digital modifications and the inherent complexities therein, the application of this criterion is especially important. Specifically, the unique aspect of concern is the potential for a software CCF to create the possibility for a malfunction with a different result. Therefore, rather than providing simplistic supplemental guidance to that already included in NEI 96-07, Section 4.3.6, more detailed guidance will be provided in this section.

Review

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

CAUTION: The following review summaries are intended for general understanding only. For complete discussions of each term, see the references identified for each term.

From NEI 96-07, Section 3.9:

> *"Malfunction of SSCs important to safety means the failure of SSCs to perform their intended **design functions** described in the UFSAR (whether or not classified as safety-related in accordance with 10 CFR 50, Appendix B)."* [***emphasis*** added]

From NEI 96-07, Section 3.3:

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

Also,

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

Furthermore,

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

Finally,

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

> *functions" refers both to those SSCs needed to support **design bases functions** (cooling, power, environmental control, etc.) and to SSCs whose operation or malfunction could adversely affect the performance of **design bases functions** (for instance, control systems and physical arrangements). Thus, both safety-related and nonsafety-related SSCs may perform design functions."* [***emphasis*** added]

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

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

1. Design bases functions are performed by SSCs that are required by, or otherwise necessary to comply with NRC requirements, or credited in the safety analyses.
2. The functions of any individual SSC are functionally below that of design bases functions.
3. Design bases functions are derived primarily from the General Design Criteria.

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

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

Then, from NEI 96-07, Section 3.12:

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

And from the first sentence of the associated discussion:

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

Also included in the definition of *safety analyses* are supporting UFSAR analyses that demonstrate that SSC design functions will be accomplished as credited in the accident analyses.

Failure Modes and Effects Analysis (FMEA)

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

From NEI 96-07, Section 4.3.6:

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

If a new/revised FMEA is determined to be needed, other effects of a digital modification could create new failure modes in addition to failures caused by software (e.g., combining functions, creating new interactions with other systems, changing response time). For example, if previously separate functions are combined in a single digital device, the failure assessment should consider whether single failures that could previously have affected only individual design functions can now affect multiple design functions.

Overall Perspective

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

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

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

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

GUIDANCE

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

Determination of "As Likely to Happen As"

From NEI 96-07, Section 4.3.6:

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

If the outcome of the *qualitative assessment* is **sufficiently low**, then the activity does not introduce any failures that are as likely to happen as those in the UFSAR. Therefore, the activity does not create a possibility for a malfunction of an SSC important to safety with a different result from any previously evaluated in the UFSAR.

If the outcome of the *qualitative assessment* is **not sufficiently low**, then the activity may introduce failures that are as likely to happen as those in the UFSAR that can create a possibility for a malfunction of an SSC important to safety with a different result from any previously evaluated in the UFSAR. For these cases, this Evaluation criterion also needs to consider the impact of this potential failure on the safety analysis result using assumptions consistent with the plant's UFSAR.

EXAMPLE

Example 4-16 illustrates the NO CREATION of the possibility for a malfunction with a different result case.

Example 4-16. NO CREATION of the Possibility for a Malfunction with a Different Result

Proposed Activity

A large number of analog transmitters in several different systems and uses are being replaced with digital transmitters. These transmitters perform a variety of functions, including controlling the automatic actuation of devices (e.g., valve stroking) that are credited in a safety analysis.

Qualitative Assessment Outcome

A *qualitative assessment* was included in the engineering/technical information supporting the change. The *qualitative assessment* considered system design attributes, quality of the design processes employed, and operating experience of the proposed equipment and concluded that the failure likelihood introduced by the modified SSCs is **sufficiently low**. For the specific items that were considered within each factor, refer to the *qualitative assessment* documented in design change package X.

Conclusion

With the failure likelihood introduced by the modified SSCs being **sufficiently low**, the activity does not introduce any failures that are as likely to happen as those in the UFSAR that can initiate a malfunction of an SSC important to safety. Therefore, the activity does not create a possibility for a malfunction of an SSC important to safety with a different result from any previously evaluated in the UFSAR (for the aspect being illustrated in this example).

Determination of Impact on ~~Safety Analysis~~Malfunction Result ~~Impact~~

For cases in which the *qualitative assessment* outcome is a failure likelihood of **not sufficiently low**, the impact on the~~*safety analysis result*~~ *of a malfunction of an SSC important to safety* ~~impact~~ needs to be assessed to determine if the result is different.

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

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

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

The functions identified as part of this step will be further classified in Step 2.

As a reminder of the guidance provided in NEI 96-07, the following additional guidance is provided to assist in the identification and consideration of the proper scope of SSCs and their functions:

1. Identification and consideration of the proper scope of SSCs is concerned with the functional involvement of an SSC, not necessarily only its level of direct description in the UFSAR.

2. In cases in which a proposed activity involves a sub-component/component that is not directly described in the UFSAR, the effect of the proposed activity involving the sub-component/component needs to consider the impact on the system in which the sub-component/component is a part.

3. In cases in which a proposed activity involves a sub-component/component that is not described in the UFSAR, the effect of the proposed activity involving the sub-component/component needs to consider the impact on the system that the subcomponent/component supports.

Regardless of the level of description, the assessment of the impact also needs to consider the elements of a design function as described in NEI 96-07, Section 3.3, which are repeated below:

- Implicitly included within the meaning of design function are the conditions under which intended functions are required to be performed, such as equipment response times, process conditions, equipment qualification and single failure.

- Design functions may be performed by safety-related SSCs or non-safety-related SSCs and include functions that, if not performed, would initiate a transient or accident that the plant is required to withstand.

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

Utilizing NEI 96-07, Section 3.3, classify each of the functions from Step 1 as either *NOT a design function* or as a *design function*.

If no *design functions* are identified, then the proposed activity does NOT create the possibility for a malfunction of an SSC important to safety with a different result because malfunctions (and the results thereof) refers ONLY to the failure of an SSC to perform its intended *design functions*.

For each *design function* identified above, utilize NEI 96-07, Section 3.3 (along with Appendix B to NEI 97-04, as needed) to separate the functions into the following categories:~~identify which *design functions* are~~

1) *design bases functions* because:

    a. they are "required by, or otherwise necessary to comply with, regulations, license conditions, orders or technical specifications"

    b. they are "credited in licensee safety analyses to meet NRC requirements"

2) ~~, which~~ *design functions* because:

    a. they "support or impact" *design bases functions* categorized as 1.a above

    b. they "support or impact" *design bases functions* categorized as 1.b above

3) ~~, and which~~ *design functions* that are not involved with *design bases functions*, but are functions that if not performed would initiate a transient or accident that the plant is required to withstand.

If multiple *design functions* are identified, each design function is to be considered individually in this multi-step process.

One means to determine if a *design function* is a *design bases function* due to category 1.a or 1.b above would be by identifying the requirement (e.g., regulation, license condition, order, or technical specification) or associated General Design Criteria (GDC) to which a *design bases function* applies or, more specifically, the associated principal design criteria (PDC) for an individual facility, the minimum standards for which are set by 10 CFR Part 50 Appendix A (or perhaps their 1967 precursors). Each *design function* may then be related to, for example, the requirements discussed within the GDC to determine if that *design function* is directly involved with the *design bases function* itself or if the *design function* "supports or impacts" the related *design bases function*. If the *design function* is found to directly involve the GDC requirement, then that *design function* is a *design bases function*. If the *design function* "supports or impacts" the GDC requirement, then it is not a *design bases function*, but is still "credited in the safety analysis."

As described in NEI 96-07, Section 4.3.2 (but equally applicable here), safety analyses typically assume certain SSCs perform certain design functions as part of demonstrating the adequacy of the design. The process of determining if a *design function* is a *design bases function* should include both direct and indirect effects on the design functions.

However, safety analyses do not typically identify all of the SSCs that are relied upon to perform their design functions. Thus, certain design functions, while not specifically identified in the safety analyses, are credited in an indirect sense. Therefore, the review should not be limited to only the SSCs discussed in the safety analyses. For example, performing a design change on a valve controller in a high pressure safety injection system would be considered to involve an SSC credited in the safety analyses even though the valve itself may not be mentioned in the safety analyses.

Finally, as described in NEI 96-07, definition 3.3, an SSC's classification as "safety-related" or "non-safety-related" is not a determining factor in identifying *design functions*. For example, a given control system may be non-safety-related but is still considered to be "credited in the safety analysis" and categorized as 2.b.

If no *design bases functions* are involved, proceed to Step 5 since neither the performance of d*esign bases functions* nor the "support or impact" of *design bases functions* are involved. (NOTE: The potential for more severe accident initiation is addressed in Step 5. These *design functions* should have been categorized as 3.)

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

If the impact on the *design bases function* involved is readily apparent, no new FMEA needs to be generated. Go to Step 4.

For example, there is no reason to contemplate the generation of a new FMEA if the impact of the failure on the *design bases functions* is recognized as being immediate. Otherwise, generate the new FMEA to describe the connection of the proposed activity, or failures due to the proposed activity, to an impact on the *design bases functions*.

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

"Interdependence" is discussed in NEI 96-07, Sections 4.2 and 4.3 (which is distinct from compensatory actions discussed in NEI 96-07, Section 4.4). An example of an interdependent procedure change would be the modifications to an existing procedure to reflect operation of the new digital equipment and controls, including any new features such as a control system restart option. (NOTE: NEI 96-07, Section 4.3.2, Example 4 provides guidance on assessing new operator actions.)

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

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

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

Step 5: Identify all ~~safety analyses~~ involved malfunctions of an SSC important to safety previously evaluated in the UFSAR.

Considering the scope of *design functions* and *design bases functions* placed into categories 1.a or 2.a from Step 2, identify all pre-existing UFSAR evaluations associated with these design functions. In addition, for those design functions placed into category 1.a or 2.a, reconsider earlier conclusions made as part of the 10 CFR 50.59 applicability determination because there may be other requirements associated with the involved design functions (e.g., a more specific change regulation, change to Technical Specifications, or change to the Operating License itself).

Considering the scope of *design functions* and *design bases functions* placed into categories 1.b and 2.b from Step 2, identify all involved malfunctions of an SSC important to safety previously evaluated in the UFSAR by identifying all safety analyses[3] that rely directly or indirectly on the *design bases functions'* performance/satisfaction.

~~Also,~~ Identify all safety analyses related to any other *design function* that could impact either the accident's initiation or the event's initial conditions (i.e., *design functions* that, if not performed, would initiate a transient or accident that the plant is required to withstand). These *design functions* should have been categorized as either 2.b or 3 as part of Step 2.

~~If there are no safety analyses involved, then there cannot be a change in the result of a safety analysis. Therefore, in this case, the proposed activity does NOT create the possibility for a malfunction of an SSC important to safety with a different result.~~

Step 6: For each ~~safety analysis~~ involved malfunction of an SSC important to safety, compare the projected/postulated results with the previously evaluated results.

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

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

For those design functions only placed into categories 1.a or 2.a (i.e., not 1.b or 2.b), assess the results of all pre-existing UFSAR evaluations and the potential for any revision to previously described results. If the results of revised evaluations are inconsistent with the "regulations, license conditions, orders or technical specifications" that were identified as part of Step 2, then the proposed activity creates the possibility for a malfunction of an SSC important to safety with a different result. (The response to criterion 2 may have already identified this inconsistency with regulations, etc.)

For those design functions placed into any other category or combination of categories, if any of the previous evaluations of involved malfunctions of an SSC important to safety ~~identified (i.e., safety analyses~~[4]) have become invalid due to their basic assumptions no longer being valid, (e.g., single failure assumption is not maintained), or if the numerical result(s) of any safety analysis would no longer satisfy the acceptance criteria,(i.e., the safety analysis is no longer bounded), then the proposed activity ~~DOES~~ creates the possibility for a malfunction of an SSC important to safety with a different result.

As part of the response and determining if the ~~safety analyses~~malfunction results continue to be bounded, include the impact on the severity of the initiating conditions and the impact on the initial conditions assumed in the associated safety analysis. Specifically, consider any *design functions* that, if not performed, would initiate a transient or accident that the plant is required to withstand. (Category 3 from Step 2.)

EXAMPLES

Commented [MP1]: NRC Comment: The language in this step will change based on OGC and NEI legal discussion and may affect language in the section 4.3.6 examples.

[3] NEI 96-07, Section 3.12, Safety Analysis
[4] ~~NEI 96-07, Section 3.12, Safety Analysis~~

Examples 4-17 through 4-21 illustrate some cases of NO CREATION of a malfunction with a different result by applying the multi-step process outlined above.

Example 4-17. NO CREATION of a Malfunction with a Different Result

Proposed Activity

A feedwater control system is being upgraded from an analog system to a digital system.

~~Safety Analysis Result~~ Impact on Malfunction Result

Step 1:

The pertinent function of the feedwater control system is to establish and maintain steam generator water level within predetermined physical limits during normal operating conditions.

Step 2:

The function of the feedwater control system is classified as a design function due to its ability to initiate a transient or accident that the plant is required to withstand. This is a category 3 design function.~~However, the design function is **not** a design bases function. With~~ Since no design bases functions are involved, proceed to Step 5.

Step 3:

Not applicable

Step 4:

Not applicable

Step 5:

The design function involved was identified as category 3. The pertinent safety analysis is the accident analysis for Loss of Feedwater. The feedwater control system has a direct impact on the accident analysis assumptions and modeling.

Step 6:

Previously, only one feedwater flow control valve (out of four) could fail closed due to a failure of the analog control system. In the proposed design, all four feedwater flow control valves could simultaneously fail closed due to a software CCF in the digital control system.

Although only one feedwater flow control valve could fail due to a failure of the analog control system, the Loss of Feedwater accident analysis assumed the closure of all four flow control valves. The severity of the initiating failure assumed in the Loss of Feedwater accident analysis (four valves affected) is unchanged since the analysis currently assumes a total loss of feedwater flow. The failure mode (valve closure) is determined to have no effect on this assumption. The mechanism by which feedwater flow is lost (loss of control signal) has no impact on the initial conditions of the event.

Conclusion

Although the software CCF likelihood was determined to be **not sufficiently low**, the initiation severity assumed in the Loss of Feedwater accident analysis (four valves affected), the failure mode (valve closure) and the mechanism by which feedwater flow was lost (loss of control signal) remain bounded.

Commented [MP2]: NRC Suggestion: This appears to be a change to a basic assumption as described in Step 6 of the guidance. Please clarify how this new failure assumption meets the guidance.

Furthermore, the results of the safety analysis, including the type of event (increasing pressure) and all criteria that must be satisfied (maximum allowed peak RCS pressure and maximum allowed secondary pressure) remain bounded.

Thus, the proposed activity does NOT create the possibility for a malfunction of an SSC important to safety with a different result (for the aspect being illustrated in this example).

Example 4-18. No CREATION of a Malfunction with a Different Result

Proposed Activity

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

~~Safety Analysis Result~~ Impact ~~Consideration~~on Malfunction Result

Step 1:

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

Step 2:

The function is classified as a design function due to its ability to "~~...~~initiate a transient or accident that the plant is required to withstand."~~.~~ This is a category 3 design function. ~~However, the design function is not a design bases function. With~~Since no design bases functions are involved, proceed to Step 5.

Step 3:

Not applicable

Step 4:

Not applicable

Step 5:

The design function involved was identified as category 3. The pertinent safety analysis is the accident analysis for Excess Feedwater. The feedwater control system has a direct impact on the accident analysis assumptions and modeling.

Step 6:

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

The minimum acceptable departure from nucleate boiling ratio (DNBR)~~, i.e., the safety analysis result,~~ is 1.30. The current safety analysis result is a minimum DNBR value equal to 1.42. After using the increased value for the new feedwater flow (to represent the increase in feedwater flow caused by the opening of the four feedwater flow control valves) in a revision to the Excess

Commented [MP3]: NRC Comment: We believe that this example is a "Creation of a malfunction with a different result" because of the reasoning that follows.

Commented [MP4]: NRC Comment: This appears to be a change to a basic assumption, as described in Step 6 of the guidance. Please clarify how this new failure assumption meets the guidance in Step 6.

Commented [MP5]: NRC Comment: In the section deleted by NRC below, was the wording supposed to be safety limit, not safety analysis result?

Commented [MP7]: NRC Comment: the minimum DNBR of 1.30 in this context appears to be an established specific fuel design safety limit for Anticipated Operational Occurrence (AOO)s to protect fuel design. Not a previously evaluated outcome of an established feedwater AOO result. The second sentence further establishes 1.42 as the previously evaluated safety analysis result.

Change of control. Malfunction of digital control system results in a change of the result. One versus four valves. You don't ever get to DNBR in this example.

Feedwater accident analysis, the new safety analysis result is a minimum DNBR value equal to 1.33.

Conclusion

Although the software CCF likelihood was determined to be **not sufficiently low** and the severity of the initiating failure has increased, a comparison of the safety analysis results of the minimum DNBR values shows that the new minimum DNBR value has decreased and does not remain~~s~~ bounded. Therefore, the proposed activity does ~~NOT~~ create the possibility for a malfunction of an SSC important to safety with a different result.

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

Proposed Activity

A complete upgrade of the area radiation monitors that monitor a variety of areas (e.g., rooms, cubicles, pipe chases, hallways) for high radiation is proposed. The outdated analog-based radiation monitors are being replaced by digital-based monitors. The hardware platform for each area radiation monitor is from the same supplier and the software in each area radiation monitor is exactly the same.

~~Safety Analysis Result~~ Impact on Malfunction Result

Step 1:

The pertinent function of each radiation monitor is to monitor the various compartments, rooms and areas that may be subject to an increase in radiation.

Step 2:

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

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

The area radiation monitors perform a function that is necessary to comply with a requirement specified in GDC 64. ~~Therefore, the function of the radiation monitor is a design function directly involved with a design bases function.~~This is a category 1.a design bases function. None of the other four categories are applicable to this function, since the radiation monitors are not credited directly or indirectly in a safety analysis~~.~~ and are not functions that if not performed would initiate a transient or accident that the plant is required to withstand.

Step 3:

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

Step 4:

Commented [MP8]: NRC Suggestion: Change added to address and track with the criteria in Step 2 of section 4.3.6.

Commented [MP9]: NRC Comment: It is not clear how the effect of a postulated CCF on high radiation monitors is readily apparent. The assumed failure could be high or low readings, or no signal, which could impact the actions taken by plant operators during normal operations or accidents.

It is not clear what "readily apparent" means.

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

Step 5:

(a) All pre-existing UFSAR evaluations associated with these design functions were identified.

The design bases function involved was only identified as category 1.a. There are no safety analyses that directly or indirectly credit this design bases function. ~~Namely, there are no considerations of malfunctions of single or multiple radiation monitors, or expected responses of the radiation monitors, in any safety analysis. Therefore, all pre-existing UFSAR described evaluations associated with these radiation monitors will be identified.~~

Step 6:

~~Not applicable~~ The design bases function involved was only identified as category 1.a. The pre-existing UFSAR described evaluations associated with GDC 64. The licensee concluded the revised result remains ~~compliance are reviewed to determine whether the revision is~~ consistent with the requirements of GDC 64.

~~In this instance, the licensee followed Regulatory Guide 1.97 to implement the requirements of GDC 64 by imposing the requirements of a "Type E" variable on these radiation monitors. The radiation monitors continue to satisfy these requirements, with the revised evaluation results remaining consistent with both GDC 64 and the requirements imposed by Regulatory Guide 1.97.~~

Conclusion

Although the software CCF likelihood was determined to be **not sufficiently low**, the revised evaluation of the radiation monitors indicates that the results remain consistent with ~~both~~ GDC 64 ~~and the requirements imposed by Regulatory Guide 1.97.~~

In addition, consistent with the design bases functions involved only belonging to category 1.a, there are no safety analyses that directly or indirectly credit the design basis function or contain expected responses of the radiation monitors. ~~Thus, there cannot be a different result when comparing to a pre-existing safety analysis since none exists.~~

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

NOTE: The acceptability of these new area radiation monitors will also be ~~dictated by their reliability, which is~~ assessed with guidance for ~~as part of~~ Criterion (ii~~), not Criterion (vi).~~

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

Proposed Activity

Two chillers that cool the Main Control Room Ventilation System (MCRVS) are being upgraded. The MCRVS provides cooling to the Main Control Room and the adjacent Relay Room. The Relay Room contains multiple instrument racks that control both the Reactor Protection System (RPS) and Engineering Safety Features Actuation System (ESFAS) signals.

As part of the upgrade, each of the chiller's analog control systems will be replaced with a digital control system. Each digital control system maintains all of the operational features (e.g.,

Commented [MP10]: NRC Suggestion: Eliminated because it is not relevant to Step 6 criteria, and is addressed above in Step 2.

Commented [MP11]: NRC Comment: The NRC is not endorsing this because it is specific technical guidance and the context it is not clear how it addresses compliance with GDC 64.

In addition, RG 1.97 also references requirements such as GDC 19 for control room habitality and 50.34(f) regarding Additional TMI-Related Requirement. It is assumed that a CCF of high radiation monitors does not impact compliance with these or other radiation protection requirements.

Commented [MP12]: NRC Suggestion: The guidance for all Criteria in NEI 96-07 and Appendix D are applicable. Criterion II does not address "reliability"

auto/manual start/stop, setpoints and alarms) as the analog control systems. The hardware platform for each chiller control system is from the same supplier and the software in each chiller control system is exactly the same.

~~Safety Analysis Result~~ Impact on Malfunction Result

Step 1:

The pertinent functions of the MCRVS involve the air flow path from the Main Control Room to the Relay Room (which is described in the UFSAR) and a function to maintain the Relay Room's temperature less than or equal to 120˚F.

Step 2:

The function involving the "air flow path" is not affected and can be eliminated from consideration since ~~the Screen phase determined that~~ there was no adverse impact.

Commented [MP13]: NRC Suggestion: Screening does not involve individual functions.

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

> *Criterion 20 -- Protection system functions. The protection system shall be designed (1)* ***to initiate automatically the operation of appropriate systems including the reactivity control systems****, to assure that specified acceptable fuel design limits are not exceeded as a result of anticipated operational occurrences and (2)* ***to sense accident conditions and to initiate the operation of systems and components important to safety****.* [***emphasis*** added]

The chiller control system performs a "maintain temperature" function that supports or impacts the design bases function specified in GDC 20. Therefore, the function of the chiller control system is a design function credited in the safety analysis. This is a category 2.b design function.

In addition, the "maintain temperature" function also performs a "support or impact" design function for the Operability of the RPS and ESFAS required per the Technical Specifications (i.e., performs a "required and necessary support function" per the definition of Operability). Thus, this is also a category 2.a design function.

Step 3:

The impact of a software CCF on the design bases function credited in the safety analysis is not readily apparent, so a new FMEA was generated.

Step 4:

The new FMEA concluded that compliance with pre-existing procedures will result in the restoration of at least one chiller well before the Relay Room cooling becomes inadequate and temperature exceeds 120˚F. Specifically, compliance with existing procedures will lead to recognition of the problem and, using currently proceduralized alternate methods for operating the system (i.e., NOT compensatory actions for addressing degraded or nonconforming conditions), restore the chiller control system function prior to the impairment of the associated design bases functions. In addition, an interdependent procedure change (satisfying the four bullets in NEI 96-07, Section 4.3.2, Example 4) will lead to the use of a new digital control system "restart" feature to reinitialize the control system and clear any software faults,

allowing the chiller control system functions to be restored well before the Relay Room cooling becomes inadequate and temperature exceeds 120˚F.

Step 5:

The design function involved was identified as categories 2.a and 2.b. Although none of the safety analyses specifically identify assumptions or inputs related to the MCRVS, the Relay Room or the components therein, several accident analyses assume correct and timely actuation of the RPS and/or the ESFAS signals. As determined in Step 2 above, a category 2.b design function indicates that the operation of the chiller control system is considered to be credited in the safety analysis since they support or impact the design bases functions associated with GDC 20. As demonstrated as part of Step 4, all design bases functions are preserved.

Step 6:

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

Conclusion

Although the software CCF likelihood was determined to be **not sufficiently low**, the design bases functions will continue to be performed/satisfied and the safety analyses (and all of the results from these analyses) are unaffected. Therefore, the proposed activity does NOT create the possibility of a malfunction of an SSC important to safety with a different result (for the aspect being illustrated in this example).

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

Proposed Activity

Currently, the non-safety-related Steam Bypass Control System (SBCS) and the non-safety-related pressurizer pressure control system are separate analog control systems.

The SBCS is being upgraded from an analog to a digital system.

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

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

~~Safety Analysis Result~~ Impact ~~Consideration~~on Malfunction Result

Step 1:

Steam Bypass - The pertinent function of the SBCS is to maximize plant availability by making full utilization of the turbine bypass valve capacity to remove NSSS thermal energy to accommodate load rejections, unit trips, and other conditions that result in the generation of excessive energy by the NSSS.

This objective is achieved by the selective use of turbine bypass valves to avoid unnecessary reactor trips and prevent the opening of secondary side safety valves whenever these occurrences can be averted by the controlled release of steam.

Pressurizer - The pertinent function is control of the pressurizer sprays and heaters to maintain RCS pressure within the established limits.

Step 2:

Steam Bypass - The function of the SBCS is classified as a design function due to its ability to initiate a transient or accident that the plant is required to withstand. This is a category 3 design function which will proceed~~However, the design function is not a design bases function. (This *design function* goes directly~~ to Step 5.~~)~~

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

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

The pressurizer control system performs a function that supports or impacts a design bases function specified in GDC 10. Therefore, the pressurizer control system function is a design function credited in the safety analysis. This is a category 2.b design function.

Step 3:

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

Step 4:

If a software CCF occurs, the pressurizer pressure control function, which supports or impacts the GDC 10 design bases function, will not be performed.

Step 5:

The design functions involved were identified as categories 2.b and 3. The pertinent safety analysis is the accident analysis for Increased Main Steam Flow. Typically, in Chapter 15 accident analyses, control system action is considered only if that action results in more severe accident results. The steam bypass and pressurizer pressure control systems have a direct impact on the accident analysis assumptions and modeling.

Step 6:

Previously, all four SBCS turbine bypass valves were assumed to fail open as part of the initiation of the Increased Main Steam Flow event. In the proposed design, all four SBCS turbine bypass valves could also fail open concurrently with the failure of the pressurizer pressure control system due to a software CCF in the digital control system.

In the Increased Main Steam Flow accident analysis, the pressurizer pressure control system is assumed to be in automatic and would attempt to mitigate the results of the accident. Initial conditions assume abnormally low pressure and the sequence of events for the accident identifies that the pressurizer empties during the event. Therefore, regardless of the operation (or mis-operation) of the pressurizer pressure control system during the event, the malfunction of the pressurizer pressure control system would have no effect on this event and no effect on the safety analysis result.

The severity of the initiating failure assumed in the Increased Main Steam Flow accident analysis (four valves affected) is unchanged since the current analysis assumes the maximum possible increased steam flow. Furthermore, the failure mode (valve closure) is determined to have no effect and the mechanism (control signal error) that allows the valves to open, allowing the steam flow to increase, has no impact on the initial conditions of the event.

The assumption regarding the "status" of the pressurizer pressure control system (i.e., automatic vs. failed) both lead to emptying of the pressurizer, having no impact on the outcome of the event.

Therefore, there are no impacts due to the combination of the two control systems.

Conclusion

Although the software CCF likelihood was determined to be **not sufficiently low**, the initiation severity assumed in the Increased Main Steam Flow accident analysis (four valves affected), the failure modes (valve closure) and the mechanism by which steam flow increases (control signal error) remain bounded. Furthermore, the results of the safety analysis, including the type of event (decreasing pressure) remain bounding because the basic assumption in the safety analyses for Main Steam Flow accident analyses subsumes postulated failure of the pressurizer control system, regardless of the mechanism of the postulated failure. ~~and all criteria that must be satisfied (maximum peak RCS pressure, maximum secondary pressure, minimum DNBR, maximum peak linear heat rate and the dose consequences) remain bounded.~~

Commented [MP14]: NRC Suggestion: Need to clarify which basic assumption this is referring to.

Commented [MP15]: NRC Suggestion: Revised to be consistent with the wording in step 6.

Therefore, the proposed activity does NOT create the possibility for a malfunction of an SSC important to safety with a different result (for the aspect being illustrated in this example).

Example~~s~~ 4-22 through 4-24 illustrate~~s a~~ some case~~s~~ in which there is the CREATION of a malfunction with a different result.

Example 4-22. CREATION of a Malfunction with a Different Result

Proposed Activity

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

~~Safety Analysis Result~~ Impact ~~Consideration~~on Malfunction Result

Step 1:

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

Step 2:

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

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

The components perform ~~functions that support or impact design bases~~ functions specified in GDCs 20, 21, and 22. Thus, these functions are design bases functions credited in the safety analysis. These are category ~~2~~1.b design bases functions.

In addition, these functions also perform a ~~"support or impact"~~ function for the Operability of the RPS per the Technical Specifications ~~(i.e., perform a "required and necessary support function" per the definition of Operability)~~. Thus, these are also category ~~2~~1.a design bases functions.

Step 3:

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

Step 4:

Commented [MP17]: NRC Suggestion: Since the guidance in Steps 5 & 6 apply nearly the identical criteria to "design functions" and "design basis functions" in some sense the distinction is not practically relevant for this guidance document, but we believe in this case it is discussing design bases functions.

The design bases functions related to the GDC 21 and 22 requirements regarding single failure criteria and redundant channels will not be performed.

Step 5:

The design bases functions involved were identified as categories ~~2~~1.a and ~~2~~1.b. Numerous safety analyses contain implicit assumptions regarding the performance and/or expectation of the minimum number of system/components and/or trains/channels that are expected to perform their function, which satisfy the applicable redundancy requirements and/or single failure criteria.

Step 6:

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

In these instances, a review of the safety analyses and their structure will quickly conclude that the results will no longer be bounded.

Conclusion

With the software CCF likelihood determined to be **not sufficiently low**, the assumptions regarding satisfaction of single failure criteria are invalidated and the results are no longer bounded. Therefore, the proposed activity CREATES the possibility of a malfunction of an SSC important to safety with a different result (for the aspect being illustrated in this example).

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

Proposed Activity

The analog voltage regulators on both trains of Emergency Diesel Generators (EDGs) are being replaced with digital voltage regulators.

~~Safety Analysis Result~~ Impact ~~Consideration~~on Malfunction Result

Step 1:

The voltage regulator is required to function properly to support EDG operation. Failure of the voltage regulator will result in failure of the associated EDG.

Step 2:

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

From GDC 17:

> *Criterion 17 -- Electric power systems.* ***An onsite electric power system*** *and an offsite electric power system shall be* ***provided to permit functioning of structures, systems, and components important to safety.*** *The safety function for each system (assuming the other system is not functioning) shall be to provide sufficient capacity and capability to assure that (1) specified acceptable fuel design limits and design conditions of the reactor coolant pressure boundary are*

not exceeded as a result of anticipated operational occurrences and (2) the core is cooled and containment integrity and other vital functions are maintained in the event of postulated accidents. [***emphasis*** added]

The function of the voltage regulator is classified as a design bases function because it ~~supports or impacts~~ performs a design bases function specified in GDC 17. Therefore, the voltage regulator's function is a design bases function credited in the safety analysis. This is a category ~~2~~1.b design bases function.

In addition, the "voltage regulation" function also performs a ~~"support or impact"~~ function for the Operability of the EDG per the Technical Specifications (i.e., performs a "required and necessary support function" per the definition of Operability). Thus, this is also a category ~~2~~1.a design bases function.

Step 3:

The effect on the voltage regulator, and the EDG's operation, is clear and understood, having a direct impact on the accident analysis assumptions and modeling. There is no reason to generate a new FMEA since the impact of the software CCF on the design basis function is readily apparent (i.e., clear and understood).

Step 4:

If a software CCF occurs, the voltage regulator's control function, which supports or impacts the GDC 17 design bases function, will not be performed.

Step 5:

The design bases function involved was identified as categories ~~2~~1.a and ~~2~~1.b. Numerous safety analyses directly credit functions that are assumed to remain powered by a single EDG, which is commonly assumed to be the limiting single failure.

Step 6:

In this instance, the basic assumption of single failure is no longer valid. Thus, if the safety analyses in question were rerun, the associated acceptance criteria would likely not be met with such a basic assumption not being maintained.

Conclusion

With the software CCF likelihood determined to be **not sufficiently low**, the assumptions regarding satisfaction of single failure criteria are invalidated and the results are no longer bounded. Therefore, the proposed activity CREATES the possibility for a malfunction of an SSC important to safety with a ~~different result.~~

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

Proposed Activity

The analog pressurizer pressure transmitters and associated circuitry used to control the Low Temperature Overpressure Protection opening signal for the pressurizer Power Operated Relief Valve (PORV) are being replaced with digital equipment.

~~Safety Analysis Result~~ Impact ~~Consideration~~on Malfunction Result

Commented [MP18]: NRC Suggestion: Same comment as in example 4-22 that discusses design functions versus design basis functions.

Commented [MP19]: NRC Comment: Verify that this wording is still valid based on the wording change in step 6 from the conversation with NRC OGC.

Step 1:

The PORVs are required to open to prevent an over pressurization of the Reactor Coolant System (RCS) when the RCS is being operated in a water-solid condition. The pressure sensing circuitry is essential to that function.

Step 2:

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

From GDC 14:

> *Criterion 14 -- Reactor coolant pressure boundary*. ***The reactor coolant pressure boundary*** *shall be designed, fabricated, erected, and tested so as to have an extremely low probability of abnormal leakage,* ***of rapidly propagating failure, and of gross rupture****.* [***emphasis*** added]

The design bases function identified in GDC 14 above applies during cold, water-solid conditions. This protection is commonly referred to as Low Temperature Overpressure Protection, or LTOP. The function of the PORV is classified as a ~~design function due to performing a function that supports or impacts a~~ design bases function specified in GDC 14. Further, the generation of an appropriate opening signal upon a high pressure condition also supports that function. Therefore, both the PORV and the pressure sensing circuitry perform design bases functions credited in the safety analysis. These are category 2.b design bases functions.

In addition, both the PORV and the pressure sensing circuitry perform a "support or impact" design function that is also a critical portion of the RCS Overpressure Protection System required by the Technical Specifications. This is a category ~~2~~1.a design bases function.

~~Specifically, the design bases function identified in GDC 14 above applies during cold, water-solid conditions. This protection is commonly referred to as Low Temperature Overpressure Protection, or LTOP. Therefore, both the PORV and the pressure sensing circuitry perform design functions credited in the safety analysis.~~

Step 3:

The effect on the pressure sensing circuitry, and the PORV's operation, is clear and understood, having a direct impact on the safety analysis assumptions and modeling. There is no reason to generate a new FMEA since the impact of the software CCF on the safety analysis is readily apparent (i.e., clear and understood).

Step 4:

If a software CCF occurs, the pressure sensing circuitry, and the PORV's operation, which perform ~~both~~ support, or impact the GDC 14 design bases function, will not be performed.

Step 5:

The design bases functions involved were identified as categories ~~2~~1.a and ~~2~~1.b. The pertinent safety analysis is typically part of the "Pressure Temperature Limits Report" (PTLR). That report is controlled by a Technical Specification in section 5.6. The PTLR itself is either summarized as part of the UFSAR or is incorporated by reference.

Commented [MP20]: NRC Suggestion: Same comment as in examples 4-22 and 4-23 that discusses design functions versus design basis functions.

Contained within the PTLR is a description of an analysis that demonstrates the selected Low Temperature PORV Setpoint will ensure RCS pressure does not exceed the limits specified in 10 CFR 50, Appendix G during a cold water-solid pressure excursion. This excursion is typically the result of an uncontrolled injection of water into the RCS via a high pressure Emergency Core Cooling System (ECCS pump).

The analysis contained within the PTLR is a safety analysis because it demonstrates that the limits contained within 10 CFR 50, Appendix G (the "acceptance criteria") for the facility's capability to withstand or respond to the LTOP excursion ("postulated event(s)") are met.

Step 6:

In this instance, the basic assumption of PORV operation is no longer valid. Thus, if the safety analyses in question were rerun, the associated acceptance criteria would likely not be met with no pressure relief capability available to mitigate the cold, overpressure transient.

Conclusion

With the software CCF likelihood determined to be **not sufficiently low**, the assumptions regarding PORV operation are invalidated and the results are no longer bounded. Therefore, the proposed activity CREATES the possibility for a malfunction of an SSC important to safety with a different result.

Commented [MP21]: NRC Comment: Verify that this wording in step 6 above is still valid based on the wording change in step 6 from the conversation with NRC OGC.

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.