S. JASON REMER
Director, Plant Life Extension

1201 F Street, NW, Suite 1100
Washington, DC 20004
P: 202.739.8112
sjr@nei.org
nei.org

Designated as original
Lyle Hefner
May 5, 2016

NUCLEAR ENERGY INSTITUTE

April 4, 2016

Mr. Lawrence Kokajko
Director, Division of Policy and Rulemaking
Office of Nuclear Reactor Regulation
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

Subject: Submittal of NEI 96-07, Appendix D, *Supplemental Guidance for Application of 10 CFR 50.59 to Digital Modifications*, Draft Revision 0

Project Number: 689

Dear Mr. Kokajko:

On behalf of the nuclear energy industry, the Nuclear Energy Institute (NEI)[1] is pleased to provide the attached draft Revision 0 of NEI 96-07, Appendix D, *Supplemental Guidance for Application of 10 CFR 50.59 to Digital Modifications*, for NRC review. This new document supplements the 10 CFR 50.59 guidance contained in NEI 96-07, Revision 1, as endorsed in Regulatory Guide 1.187, for focused application to activities involving digital modifications. Specifically, this draft revision is intended to supersede the guidance for implementing 10 CFR 50.59 for digital modifications that was previously contained in NEI 01-01, *Guideline on Licensing Digital Upgrades: EPRI TR-102348, Revision 1.*

By letter dated November 5, 2013,[2] the NRC expressed concerns with NEI 01-01. To resolve those concerns, the NRC and industry have participated in a series of meetings over the last two-and-a-half years. One clear source of confusion in the implementation of NEI 01-01 was the appearance that it contained considerable technical guidance applicable to digital modifications. With the creation of NEI 96-07, Appendix D, the industry intends to be clear that this guidance is strictly for the application of the 10 CFR 50.59 process. Examples in NEI 96-07, Appendix D, provide enough technical detail to understand the digital modification under review and clearly specify that conclusions about the technical adequacy of the digital modification are expected to be documented elsewhere, i.e., in an engineering evaluation. NEI 96-07, Appendix D, does

[1] NEI is the organization responsible for establishing unified nuclear industry policy on matters affecting the nuclear energy industry, including the regulatory aspects of generic operational and technical issues. NEI's members include all utilities licensed to operate commercial nuclear power plants in the United States, nuclear plant designers, major architect/engineering firms, fuel fabrication facilities, materials licensees, and other organizations and individuals involved in the nuclear energy industry.

[2] NRC Letter from Mr. John Thorp to Mr. Anthony R. Pietrangelo, Nuclear Energy Institute, dated November 5, 2013.

D046

not specify what technical guidance is to be followed for engineering digital modifications; that decision is left to the licensee. One technical guidance option for licensees is EPRI 3002005326, *Methods for Assuring Safety and Dependability when Applying Digital Instrumentation and Control Systems*, but, again, no particular technical guidance document is specified as a prerequisite for use of NEI 96-07, Appendix D.

We believe that NEI 96-07, Appendix D, addresses the NRC concerns related to the 10 CFR 50.59 process guidance in NEI 01-01 and provides examples that will facilitate application of technical evaluation results in response to 10 CFR 50.59 reviews for digital modifications. Upon resolution of any staff comments on draft NEI 96-07, Appendix D, Revision 0, we plan to submit the final guidance for NRC endorsement in a regulatory guide. Licensees would like to begin using this guidance as soon as possible; as such, we request NRC staff comments on the attached draft within 60 days.

If there are any questions on this matter, please contact me or Kati Austgen (202.739.8068; kra@nei.org).

Sincerely,

S. Jason Remer

Attachment

c: Mr. John W. Lubinski, NRR/DE, NRC
Mr. David P. Beaulieu, NRR/DPR/PGCB, NRC
Ms. Deirdre Spaulding-Yeoman, NRR/DE/EICB, NRC
Mr. Norbert Carte, NRR/DE/EICB, NRC
Mr. Steven A. Arndt, NRR/DE, NRC
Mr. Joseph Holonich, Jr., NRR/DPR/PLPB, NRC
Mr. Paul J. Rebstock, Jr., RES/DE/ICEEB, NRC
Mr. Dinesh Taneja, NRO/DEIA/ICE, NRC
Mr. Richard J. Stattel, NRR/DE/EICB, NRC
Mr. Robert Austin, EPRI
NRC Document Control Desk

NEI 96-07, Appendix D
Draft Revision 0

Nuclear Energy Institute

SUPPLEMENTAL GUIDANCE FOR APPLICATION OF 10 CFR 50.59 TO DIGITAL MODIFICATIONS

April 2016

ACKNOWLEDGMENTS

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

NOTICE

EXECUTIVE SUMMARY

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

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

The guidance in this appendix supersedes NEI 01-01/ EPRI TR-102348, Guideline on Licensing of Digital Upgrades.

TABLE OF CONTENTS

1 INTRODUCTION

CAUTION

The guidance contained in this appendix is intended to supplement the generic guidance contained in the main body in NEI 96-07, Revision 1. Namely, the generic guidance provided in the main body of NEI 96-07 and the more-focused guidance in this appendix BOTH apply to digital modifications.

1.1 BACKGROUND

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

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

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

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

EPRI document 3002005326, *Methods for Assuring Safety and Dependability when Applying Digital Instrumentation and Control Systems*, has been created to provide technical guidance for the development and design of digital systems with the purpose of systematically identifying, assessing, and managing failure susceptibilities of I&C systems and components. However, the use of EPRI

3002005326 is not required for the application of the 50.59-related guidance in this appendix.

1.2 PURPOSE

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

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

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

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

2 DEFINITIONS

This section provides definitions for key terms that are important when using this appendix, and supplement those terms defined in the main body of NEI 96-07, Section 3.

2.1 **Common Cause Failure (CCF):** Postulated or actual concurrent failures where the first and second or multiple failures occur within a time interval that is less than that to detect the first failure and prevent subsequent failures of multiple systems, structures or components (SSCs) possessing the same undetected defect that manifests itself from a single event or cause. A single event or cause can be from a software defect, hardware failure, maintenance activity error, or an unanticipated consequence of combining multiple systems or components that previously functioned separately.

2.2 **Common Cause Failure Susceptibility Analysis:** An analysis that considers potential failure sources within an I&C system and identifies any existing preventive measures or limiting measures for each failure source. This analysis also identifies the SSC failure(s) caused by an I&C failure if the likelihood of the SSC failure(s) is not sufficiently low for each specific failure source.

There are two possible conclusions from a CCF Susceptibility Analysis: "CCF Unlikely" and "CCF Not Unlikely" (See separate definitions for each conclusion.)

2.3 **Common Cause Failure Susceptibility Analysis Conclusions:**

(1) "CCF Unlikely" (Technical Conclusion): Obtained from the CCF Susceptibility Analysis, a technical conclusion of "CCF Unlikely" is equivalent to a licensing condition of *NOT credible* and/or *NOT as likely to happen as those malfunctions previously considered and/or described in the UFSAR.*

(2) "CCF Not Unlikely" (Technical Conclusion): Obtained from the CCF Susceptibility Analysis, a technical conclusion of "CCF not unlikely" is equivalent to a licensing condition of *credible* and/or *as likely to happen as those malfunctions described in the UFSAR.*

2.4 **Coping Analysis:** An analysis that shows whether the mitigative measures are adequate to manage the undesirable effects of a failure (or misbehavior or CCF), assuming the measures that are in place to prevent the failure are not effective.

2.5 **Data**: A representation of facts, concepts, or instructions in a manner suitable for communication, interpretation, or processing by humans or by automatic means.

2.6 **Dependability:** A broad concept incorporating various characteristics of digital equipment, including reliability, safety, availability, and maintainability. This term reflects the notion that assurance of adequate quality and low likelihood of failure is derived from a qualitative assessment of the design process and the system design features.

The term *dependability* also reflects the importance of ensuring that the system performs its functions in a consistent and repeatable manner and its behavior is predictable. A *reliable* system that performs its intended function, but exhibits other undesirable behaviors, is not *dependable.*

2.7 **Digital modification**: A modification to a plant system or component which involves computers, computer programs, data (and its presentation), embedded digital devices, software, firmware, hardware, the human-system interface, microprocessors and programmable digital devices (e.g., Programmable Logic Devices and Field Programmable Gate Arrays). These modifications are often made to plant instrumentation and control (I&C) systems, but the term as used in this document also applies to mechanical or electrical equipment when the new equipment contains a computer (e.g., installation of a new heating and ventilation system which includes controls that use one or more embedded microprocessors).

2.8 **Hazard Analysis:** (1) A process that explores and identifies conditions that are not identified by the normal design review and testing process. The scope of hazard analysis extends beyond plant *design basis* events by including abnormal events and plant operations with degraded equipment and plant systems. Hazard analysis focuses on system failure mechanisms rather than verifying correct system operation; (2) The process of identifying hazards and their potential causal factors. Conceptually, "hazard analysis" may be considered somewhat broader than "failure analysis" in the sense that it also considers situations in which there can be losses in the absence of any failures of systems, subsystems or components. This document uses the two terms interchangeably in the broader context.

2.9 **Human-System Interface (HSI):** All interfaces between the digital system and plant personnel including operators, maintenance technicians, and engineering personnel (e.g., display or control interfaces, test panels, configuration terminals, etc.). These interfaces include information and control resources used by plant personnel to perform their duties and tasks. Currently, HSI is the term that is synonymous with and replaces human-machine interface (HMI) and man-machine interface (MMI). Principal HSIs

are: alarms, information displays and controls. A HSI may be made up of hardware and software components and is characterized in terms of its physical and functional characteristics.

2.10 Layers of Design: This phrase will be used in the Screen Phase (Section 3) discussion regarding the consideration of possible adverse effects due to the combination of components and/or functions and refers to a licensing concept. Examples of *layers of design* are *independence* (e.g., two components with no commonality), *separation* (e.g., different physical locations or use of individual components), *redundancy* (e.g., duplication of equipment) and multiple sources (e.g., multiple electrical power sources, such as normal off-site power, and emergency on-site power provided by diesel generators and batteries; or multiple cooling water sources, such as normal make-up tanks, fire water tanks, refueling water tanks, cooling tower ponds and emergency off-site sources such as lakes, rivers and ponds).

2.11 Variety: This word will be used in the Screen Phase (Section 3) discussion regarding the consideration of possible adverse effects due to the combination of components and/or functions and refers to a licensing concept. An example of *variety* as a licensing concept is that a facility may have both *motor-driven* and *steam-driven* auxiliary feedwater pumps.

3 SCREEN GUIDANCE

CAUTION

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

3.1 INTRODUCTION

There is no regulatory or technical requirement for a proposed activity involving a digital modification to *default* (i.e., be mandatorily "forced") to having an adverse effect on how a UFSAR-described design function is performed or controlled. The introduction of software or digital hardware, in and of itself, does not cause the proposed activity to be adverse (i.e., "screen in"). Likewise, simply because software and/or digital hardware is replaced with other software and/or digital hardware does not cause the proposed activity to be adverse.

Similarly, a proposed activity involving a digital modification does not necessarily involve a fundamental change in how a design function is performed.

Examples 3-1 and 3-2 illustrate the relationship between a digital modification and the concept of a fundamental change in how a design function is performed.

Example 3-1. Digital Modification that does NOT contain a Fundamental Change to How a Design Function is Performed or Controlled

Flow in a system is measured using a venturi (which generates a differential pressure signal that is described in the UFSAR) and the instrumentation loop contains analog components (which are not described in detail in the UFSAR). If all of the analog components (except for the venturi itself) are replaced with digital components and/or a digital control system, but flow is still developed using the differential pressure signal, there is no change in how the design function (i.e., measuring flow) is performed.

The use of digital equipment (hardware and software) still needs to be addressed in the Screen to determine the impact on the pertinent design functions, but not as a "fundamental" change.

Example 3-2. Digital Modification that DOES contain a Fundamental Change to How a Design Function is Performed or Controlled

Main feedwater flow to the steam generators is manually controlled by the licensed Operators, who use steam generator level to determine if flow should be adjusted. There are two separate and independent analog controls systems (one for each main feedwater pump) that do not interact or communicate in any manner. All of these features (i.e., manual operation, adjustments based on level and two separate control systems) are described in the UFSAR. Two new digital feedwater control systems will replace the analog control systems, maintaining the original separation provided by the analog systems. The new control systems will automatically control feedwater flow and will use steam generator *level* and steam generator *pressure* to determine the proper flow rate.

In this case, there are two activities that "fundamentally alter how a design function is performed:" (1) *manual-to-auto* and (2) *level-only to level-and-pressure.*

Note that the use of digital equipment (hardware and software) is not the source of the fundamental changes; it was the *manual-to-auto* and *level-only to level-and-pressure* activities that were the fundamental changes.

3.2 PROCESS

To determine if adverse impacts on UFSAR-described design functions have been created, the 10 CFR 50.59 Screen for a digital modification should consider two possible aspects of the proposed activity:

- Software/Hardware
- Human-System Interface

The first aspect (Software/Hardware) will be considered as a proposed activity affecting the ***facility*** (see main body NEI 96-07, Section 3.6), involving structures, systems and components (SSCs) and their associated UFSAR-described design functions. The second aspect (Human-System Interface) will be considered a proposed activity affecting ***procedures*** (see main body NEI 96-07, Section 3.11), specifying how UFSAR-described design functions are performed or controlled.

The Screen guidance in this appendix is arranged in sections paralleling that used in section 4.2 of the main body of NEI 96-07.

3.2.1 SCREENING OF CHANGES TO THE FACILITY AS DESCRIBED IN THE UFSAR

3.2.1.1 SCOPE

The screening of proposed activities involving the *facility as described in the UFSAR* considers the software and hardware portions of the digital modification.

3.2.1.2 COMBINATION OF COMPONENTS/FUNCTIONS

During the original licensing process, the number of components, how the components were arranged, and/or how functions were allocated to those components, may have been a consideration that provided a level of physical and/or functional variety and/or layers of design.

When replacing analog SSCs, it is potentially advantageous to combine multiple components and/or functions into a single device or control system. However, the failure of the single device or control system for any reason (e.g., software defect, hardware failure, environmental effects, etc.) can potentially affect multiple functions.

To assist in determining the impact of a digital modification on the number and/or arrangement of components, review the description of the existing system(s) and/or component(s) in the UFSAR and compare how the number and/or arrangement of components is reflected in the proposed number and/or arrangement of components. Typically, drawings included as part of the UFSAR or those considered to be *incorporated by reference* (see main body NEI 96-07, Section 3.7) will show the current configuration as having a specific number and/or a specific arrangement of components. Using the current configuration, consider how the proposed configuration affects variety and/or layers of design.

If the combination of components and/or functions does not involve SSCs described in the UFSAR (directly or indirectly), or does not involve UFSAR-described design functions, then there cannot be an adverse impact due to the combination aspect of the digital activity.

Alternately, if the affected SSCs are described in the UFSAR and/or the design functions of the affected SSCs are described in the UFSAR, then the determination of the impact of an activity involving a digital modification that combines components and/or functions considers if the activity reduces existing variety and/or layers of design.

The combination of previously separate components and/or functions, in and of itself, does not make the Screen conclusion adverse. Only if combining the

previously separate components and/or functions causes a reduction in the reliability of performing a design function (e.g., by the creation of a new malfunction or the creation of a new accident initiator) is the combination aspect of the digital activity adverse.

Examples 3-3 through 3-7 illustrate possible impact(s) on design functions for different digital modifications due to the combination of components and/or functions.

Example 3-3. Combining Components and Functions that Does NOT Cause an Adverse Impact on a UFSAR-Described Design Function

A licensee has two non-safety-related main feedwater pumps (MFWPs) that were originally designed with identical analog control systems. Each analog control system has many subcomponents performing dedicated functions.

To manage obsolescence and improve reliability, the licensee proposes to replace all of the analog subcomponents with a digital device that consolidates all of the components, sub-components and the functions associated with each component and sub-component into a digital device. Each analog control system will be replaced with a separate digital control system. There are no interactions between the two new digital control systems or any other plant component(s) that did not previously exist.

Only the control system is described in the UFSAR, not the individual components or subcomponents. The loss of all feedwater to the steam generators due to the loss of both analog control systems has been previously considered in the licensing basis. Furthermore, the maximum output from both feedwater pumps has been previously considered in the licensing basis as a conservative assumption in the applicable accident analysis.

Since only the control system is described in the UFSAR, it is the only SSC to be examined for the identification of design functions. The control system contains a design function "to provide adequate cooling water to the steam generators during normal operation." This function rises to the level of a design function because, if not performed, the inability to provide cooling water to the steam generators would initiate a transient or accident that the plant is required to withstand (i.e., Loss of Feedwater).

The combination of components and functions has NO adverse impact on the identified design function for several reasons:

(1) No design functions for any of the sub-components are described in the UFSAR. Since no design functions are described for a particular SSC, then no adverse

impacts can occur.
(2) Because the entire feedwater control system is non-safety-related, there is no regulatory requirement to provide redundancy. The two control systems existed for operational convenience only, not to satisfy any General Design Criteria requirements.
(3) There is no reduction in the credited variety since none originally existed or was described in the UFSAR.
(4) There is no deviation from, or reduction in, the separation or independence as described in the UFSAR. Each of the analog control systems will be replaced with its own digital control system.
(5) No new malfunctions are created. Since no new malfunctions are created, the ability to perform the design function "to provide adequate cooling water to the steam generators during normal operation" is not adversely impacted.

Example 3-4. Combining Components and Functions that does NOT Cause an Adverse Impact on a UFSAR-Described Design Function

Using the same initial facility configuration from Example 3-3, this example illustrates how a variation in the proposed activity would be addressed.

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

Although the UFSAR explicitly describes the existence of two control systems, combining the two analog control systems into one digital control system is NOT adverse because no new malfunctions are created (i.e., recall that the loss of both control systems and maximum feedwater flows from both feedwater pumps have already been considered in the licensing basis). Since no new malfunctions are created, the reliability of the design function "to provide adequate cooling water to the steam generators during normal operation" is not adversely impacted.

Example 3-5. Combining Components and Functions that DOES Cause an Adverse Impact on a UFSAR-Described Design Function

Using the same initial facility configuration and proposed activity (i.e., use of two separate and independent digital control systems) from Example 3-3, this example illustrates how a variation in the licensing basis as described in the UFSAR impacts the Screen conclusion, causing an adverse impact.

Instead of the loss of all feedwater to the steam generators due to the loss of both analog control systems being previously considered in the licensing basis, the loss of

only one analog control system (and its worst-case affect on feedwater flow) has been considered.

In this case, the proposed activity would be adverse since a new malfunction is created (i.e., loss of both control systems) due to a CCF (e.g., a software defect in both digital control systems).

Similarly, if the combination of components and functions examined in Example 3-4 was proposed (i.e., use of only one digital control system), the proposed activity would be adverse for the same reason as above (i.e., creation of a new malfunction).

In both cases, the adverse impact is due to the reduction in the reliability of the design function "to provide adequate cooling water to the steam generators during normal operation."

Example 3-6. Combining Components and Functions that DOES Cause an Adverse Impact on a UFSAR-Described Design Function

Using the same initial facility configuration from Example 3-3, this example illustrates how a significant variation in the proposed activity would cause an adverse impact.

In addition to the feedwater control systems, the licensee has several non-safety-related main turbine steam-inlet valves that are controlled with a single analog control system. The main turbine steam-inlet valves analog control system has many subcomponents performing dedicated functions. However, only the main turbine steam-inlet valves control system is described in the UFSAR, not the individual components or subcomponents.

To manage obsolescence and improve reliability, the licensee proposes to combine the feedwater control systems and the turbine steam-inlet valves control system into one digital device.

The design function for the feedwater control system from Example 3-3 remains pertinent. Since only the turbine steam-inlet control valve control system is described in the UFSAR, it is the only SSC to be examined for the identification of design functions. The turbine control system contains a design function "to control the amount of steam entering the main turbine during normal operation." This function rises to the level of a design function because, if not performed, the inability to control steam to the main turbine would initiate an accident (i.e., Excess Steam Demand or Loss of Load).

The loss of all feedwater to the steam generators due to the loss of both analog

control systems has been previously considered in the licensing basis (i.e., the Loss of Feedwater accident).

The failure of all the steam-inlet valves (e.g., all valves going fully closed or all valves going fully open) due to the loss of the analog control system has been considered in the licensing basis, as follows: "all open" is considered in the Excess Steam Demand accident and "all closed" is considered in the Loss of Load accident.

The licensing basis does not consider the combination of the Loss of Feedwater accident with either the Excess Steam Demand accident or the Loss of Load accident.

In this case, the proposed activity would be adverse because a new malfunction has been created (i.e., loss of both feedwater control systems and the loss of the turbine control system) that was not previously considered in the licensing basis.

Furthermore, the combination of the different control systems causes a reduction in the variety described in the UFSAR.

These impacts have an adverse impact on reliability of the feedwater control system design function "to provide adequate cooling water to the steam generators during normal operation" and the reliability of the turbine control system design function "to control the amount of steam entering the main turbine during normal operation."

Example 3-7. Combining Functions that DOES Cause an Adverse Impact on a UFSAR-Described Design Function

A design function in a Pressurized Water Reactor is to provide auxiliary (or emergency) feedwater (AFW) to the steam generator(s) following a reactor trip to remove decay heat and bring the reactor to a cold shutdown condition. The UFSAR describes the facility as providing the auxiliary feedwater supply function by two redundant trains of motor-driven AFW pumps (MDAFWPs), and a non-redundant steam turbine-driven AFW pump (TDAFWP) that will provide the function even with both trains of emergency power not available to the MDAWFPs.

Plant Technical Specifications include limiting conditions for operation for both the MDAFWPs and the TDAFWP. This level of variety is clearly credited in the facility's licensing basis.

Any digital activity attempting to reduce this level of variety (e.g., installing a digital control system that included control of both the MDAFWPs and the TDAFWP) would have an adverse impact on the UFSAR-described design function.

3.2.1.3 COPING ANALYSES

A coping analysis is one possible method of providing additional assurance of adequate protection should a SSC malfunction from a CCF. The coping analysis evaluates the plant-level effect of a failure that causes a malfunction of one or more SSCs, with the objective of demonstrating additional assurance that the plant remains safe, despite the malfunction.

If the coping analysis involves re-running a safety analysis, the guidance from the main body of NEI 96-07, Section 4.2.1, subsection titled "Screening for Adverse Effects," applies for determining if the Screen can use the analysis result as a basis for a not adverse conclusion or if the Screen conclusion must be considered to be adverse.

If the coping analysis involves modifications to how SSCs will be designed or how the facility will be operated, then those modifications are additional activities that need to be addressed in the Screen (and Evaluation, if adverse impacts are identified).

3.2.1.4 DEPENDABILITY

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

> "...a change that decreases the reliability of a [design] function whose failure could initiate an accident would be considered to adversely affect a design function..."

For digital modifications, the most commonly used term to describe this concept is "dependability." To address dependability of a design function for an activity involving a digital modification, the following tools may be used:

- Operating History of the Hardware and/or Software
- Development (including design attributes and the process), Testability, Verification & Validation (V&V), and Configuration Management of the Hardware and/or Software
- Design Measures (including data validation, cyclic software architecture, internal redundancy, etc.).

To address dependability, the Screen should contain a discussion of the information (including the identification of associated references) gathered from applying the tools identified above.

Typically, digital equipment is more reliable than the equipment it replaces and often incorporates design features that contribute to a lower likelihood of malfunction. Such features can improve the dependability of a train of a system; thus preserving the system-level design function. These features should be identified in the response to this Screen consideration, and may include discussions of the following attributes and/or characteristics:

- Internal redundancy and fault tolerance to preclude single faults from causing the device to malfunction.
- Self-diagnostics to detect and alarm faults, or abnormal or unanticipated conditions so that operators can take timely corrective action before the system is called upon to perform its design function.
- Self-test routines that perform surveillance testing functions on a more frequent basis than the original, manually executed surveillance tests.
- Preventive measures
- System performance under high duty cycle loading (e.g., computational burden during accident conditions).
- Availability of a means to alert the operators to the failure condition.

3.2.2 Screening of Changes to Procedures as Described in the UFSAR

3.2.2.1 Scope

The screening of proposed activities involving *procedures as described in the UFSAR* considers the Human-System Interface portion of the digital modification.

The focus of the Screen is on potential adverse effects due to modifications of the *interface* between the human user and the technical device, not the written procedure modifications that may accompany a physical design modification.

3.2.2.2 Physical Interface

Physical Interaction

Consideration of the digital modification on the impact on the physical interaction does NOT include the items identified in the main body of NEI 96-07, Section 4.2.1.2 (e.g., equipment manipulations, actions taken or options available, manipulation sequences or operator response times). None of these items are unique to activities involving digital modifications. If any of these items are part of the

digital modification, they would be addressed separately in the Screen using the guidance in the main body of NEI 96-07, Section 4.2.1.2.

Consideration of the digital modification on the impact on physical interaction involves an examination of the actual physical interface and how it could impact the performance and/or satisfaction of UFSAR-described design functions. For example, if a new malfunction is created as a result of the physical interaction, then the HSI portion of the digital modification would be adverse. Such a new malfunction may be created by the interface requiring the human user to choose which of multiple components is to be controlled, creating the possibility of selecting the wrong component (which could not occur with an analog system that did not need the human user to make a "selection"). Example 6 (in Section 5) illustrates this concept at the end of the response to this Screen consideration in the sub-section titled "*ALTERNATE Conclusions and Justifications for Physical Interface Assessment - Physical Interaction.*"

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

To determine possible impacts, the UFSAR must be reviewed to identify descriptions regarding how the interaction with the current component or system is described and how that interaction contributes to UFSAR-described design functions being performed and/or satisfied.

A typical physical interaction modification might involve use of a touch screen in place of push-buttons, switches or knobs. The digital aspect is concerned with the interaction itself, not how the physical component is operated and controlled.

Example 3-8. Physical Interaction that does NOT Cause an Adverse Impact on a UFSAR-Described Design Function

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

The UFSAR states that the operator can "increase and decrease the control functions using manual controls located in the Main Control Room."

Examining only the digital modification aspect (i.e., ignoring the impact on operator response time or the number and/or sequence of steps necessary to access the new digital controls), the replacement of the "knob" with a "touch screen" is not adverse

since it does not adversely impact the ability of the operator to "increase and decrease the control functions using manual controls located in the Main Control Room."

Example 3-9. Physical Interaction that DOES Cause an Adverse Impact on a UFSAR-Described Design Function

Using the same proposed activity described in Example 3-8, this example illustrates how a variation in the UFSAR description would cause an adverse impact.

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

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

Example 3-10. Physical Interaction that DOES Cause an Adverse Impact on a UFSAR-Described Design Function

Using the same proposed activity described in Example 3-8 and the same UFSAR descriptions from Example 3-9, this example illustrates how a variation in the proposed activity would also cause an adverse impact.

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

Although the operator will now receive "feedback" during the operation of the digital device, the fundamental means by which this feedback is provided has been altered (See Example 3-2 also). Since the fundamental means of controlling the design function has changed, new malfunctions can be postulated. Therefore, the modification of the feedback feature (i.e., from tactile to auditory) has an adverse impact on how the design function is performed.

Number and/or Type of Parameters

Potential impacts due to the modification of the number and/or type of parameters monitored should be addressed. The purpose of addressing this factor is to determine if the number and/or type of information available due to a digital modification causes an adverse impact on the performance and/or satisfaction of a UFSAR-described design function.

A reduction in the number of system parameters monitored (which could make the diagnosis of a problem or determination of the proper action more challenging or time-consuming to the operator), the absence of a previously available parameter (i.e., a type of parameter), or a difference in how the loss (or failure) of parameters occurs (e.g., as the result of combining parameters), could potentially cause an adverse impact on a UFSAR-described design function.

To determine possible impacts, the UFSAR must be reviewed to identify descriptions regarding which information is necessary for a UFSAR-described design function to be performed and/or satisfied.

Example 3-11. Number and Type of Parameters that do NOT Cause an Adverse Impact on a UFSAR-Described Design Function

A UFSAR states that the operator will "examine pump response and utilize redundant plant channels to verify performance." This statement means that parameters *directly* associated with the pump (e.g., motor electrical current, discharge pressure and flow rate) and parameters *indirectly* associated with pump performance (e.g., response of redundant temperature indications or response of redundant level indications, as appropriate) are necessary to validate correct pump operation.

A new digital system presents the same number ("three") and type ("motor electrical current, discharge pressure and flow rate") of parameters. Furthermore, the new digital system presents the same indirect redundant information to the operator

Therefore, there is no adverse impact on the UFSAR-described ability to perform *direct* monitoring of pump performance and no adverse impact on the UFSAR-described ability to perform *indirect* monitoring of pump performance.

Information Presentation

Potential impacts due to the modification of how information is presented should be addressed.

The purpose of addressing this factor is to determine if the method by which information is presented due to a digital modification causes an adverse impact on the performance and/or satisfaction of a UFSAR-described design function.

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

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

Adverse effects may result from the following impacts:

- An increase in the number and/or type of parameters available for observation.
- Addition or removal of a dead-band
- Replacement of instantaneous readings with time-averaged readings (or vice-versa).

Example 3-12. Information and Data Presentation that DOES Cause an Adverse Impact on a UFSAR-Described Design Function

Using the pump example introduced in Example 3-8 above, the UFSAR describes a presentation method as consisting of "indicators with a 10 gpm increment" and the physical layout as being "by flow path" (i.e., not by channel/train).

A digital modification consolidates the information and controls on two flat panel displays (one for each redundant channel/train), each with a touch screen providing "soft" control capability. Also, due to the increased precision of the digital equipment, the increment of presentation will be improved to 1 gpm.

Two specific considerations due to the modification in data presentation include:

- A fundamental change in how the information is presented to the operator (by *channel/train* instead of by *flow path*).

- An increase in the precision of the information being provided (e.g., from the original "10 gpm increments" to "1 gpm increments").

Since the UFSAR describes a design function related to the *flow-path* approach, this portion of the proposed activity is adverse (i.e., the difference in presentation approach is fundamentally different than that described in the UFSAR). However, the increase in the display increment is not adverse since the operator will continue to be able to distinguish the minimum increment of 10 gpm as described in the UFSAR.

3.2.3 Screening of 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 main body 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 main body NEI 96-07, Section 3.10) resulting from a digital modification is separate from the digital modification itself and the guidance in the main body of NEI 96-07, Section 4.2.1.3 applies.

3.2.4 Screening of 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 main body NEI 96-07, Section 4.2.2). The response to this Screen consideration should reflect this characterization.

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

4 EVALUATION GUIDANCE

CAUTION

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

4.1 DOES THE ACTIVITY RESULT IN MORE THAN A MINIMAL INCREASE IN THE FREQUENCY OF OCCURRENCE OF AN ACCIDENT?

Common Cause Failure Considerations

For the special case in which a malfunction is also an accident initiator, the conclusion from the CCF Susceptibility Analysis (i.e., *CCF Unlikely* or *CCF Not Unlikely*) and the impact thereof examined in Evaluation criterion #2 (See Section 4.2) has a link to the response for Evaluation criterion #1. Namely, if the response to Evaluation criterion #2 concludes that there is no discernible increase in the likelihood of the malfunction, then there is a corresponding conclusion that there is no discernible increase in the frequency of the accident initiated by that malfunction.

Use of Probable Risk Assessment (PRA)

This is the only Evaluation criterion in which PRA information may be used during the development of a response for the impact on accident frequency. However, the use of PRA remains subject to the guidance and restrictions contained in NEI 96-07, Section 4.3.1.

4.2 DOES THE ACTIVITY RESULT IN MORE THAN A MINIMAL INCREASE IN THE LIKELIHOOD OF OCCURRENCE OF A MALFUNCTION OF AN SSC IMPORTANT TO SAFETY?

4.2.1 GENERAL CONSIDERATIONS

Level of Detail

Determining the correct UFSAR-described level of detail is especially important for digital modifications because components and/or functions may be combined, affecting how the likelihood of a malfunctions described in the UFSAR could be impacted.

Hazard Analysis

The Hazard Analysis performed during the design effort is needed to understand how potential failures of the digital modification affect the system in which it is installed and/or the component(s) involved, and whether the malfunctions due to digital device failures impact the malfunctions that are described in the UFSAR at the same level of detail. The Hazard Analysis will assist in providing insights into determining if a reduction in redundancy, diversity, separation, or independence causes an attributable and discernible increase in the likelihood of occurrence of a malfunction previously evaluated in the UFSAR.

Common Cause Failure Considerations

A CCF Susceptibility Analysis will provide the necessary information and conclusions to determine which outcomes exist for the software and hardware portions of the digital modification under consideration. There are two possible conclusions from a CCF Susceptibility Analysis: *CCF Unlikely* or *CCF Not Unlikely*.

4.2.2 APPLICATION OF GUIDANCE

Software developed and hardware designed in accordance with a defined process, complying with the applicable industry standards and regulatory guidance does not result in more than a minimal increase in the likelihood of a malfunction.

For digital equipment that has undergone commercial grade dedication (CGD), the equipment is considered essentially equivalent to compliance with the regulatory guidance and industry standards normally applicable to safety-related digital

equipment. Although there exists relatively little regulatory guidance for non-safety-related digital equipment, a graded approach for application to non-safety-related digital equipment can provide a significant reduction in the likelihood of a malfunction.

For purposes of 50.59, a conclusion of *CCF Unlikely* is equivalent to a licensing condition of a CCF malfunction being not credible. If a malfunction due to a CCF is not credible, then there is not more than a minimal increase in the likelihood of occurrence of malfunctions previously evaluated in the UFSAR due to a CCF.

Alternately, for purposes of 50.59, a conclusion of *CCF Not Unlikely* is equivalent to a licensing condition of a CCF malfunction being credible. If a malfunction due to a CCF is credible, then the impact on the likelihood of a malfunction previously considered in the UFSAR needs to be determined. However, for the *CCF Not Unlikely* conclusion, an increase in the likelihood of the malfunction occurring may or may not be "discernible" (refer to the "discernible and attributable" discussion in Section 4.3.2 of the main body of NEI 96-07).

4.3 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 the main body of NEI 96-07, Section 4.3.3 applies.

4.4 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 the main body of NEI 96-07, Section 4.3.4 applies.

4.5 DOES THE ACTIVITY CREATE A POSSIBILITY FOR AN ACCIDENT OF A DIFFERENT TYPE?

Note: In the following discussions, the word "train" shall be assumed to include "channel" and "division," and any other designator used to describe redundant components and/or systems.

4.5.1 GENERAL CONSIDERATIONS

Common Cause Failure Considerations

A CCF Susceptibility Analysis will provide the necessary information and conclusions to determine which outcomes exist for the software and hardware portions of the digital modification under consideration. There are two possible conclusions from a CCF Susceptibility Analysis: *CCF Unlikely* or *CCF Not Unlikely*.

Initiation of Multiple Accidents

The following is an excerpt from a UFSAR:

> Accident - Any natural or accidental event of infrequent occurrence and its related consequences which affect the plant operation and require the use of ESF. Such events, ***analyzed independently and not assumed to occur simultaneously***, include the loss-of-coolant accident (LOCA), steam line ruptures, steam generator tube ruptures, etc. A loss of normal (main generator) and all offsite ac power may be an isolated occurrence or may be concurrent with any event requiring ESF use if the event should cause turbine trip and grid failure. [**bold italic emphasis added**]

Even if such an explicit discussion is not provided in a licensee's UFSAR, it is clear by reviewing each of the accidents that are included in any UFSAR that only one accident is assumed to occur at a time, excluding the Loss of Offsite Power (LOOP) assumption that must be applied for some accidents. Therefore, the initiation of more than one accident due to any reason (including a CCF) creates an accident of a different type.

HSI Considerations

Recalling the HSI factors that were addressed in the Screen that could lead to potential adverse impacts (i.e., physical interaction, the number and/or type of parameters monitored, and information presentation), they may need to be considered here.

Physical Interaction

If an adverse impact resulted from the physical interaction with the digital system/component, human error would be the potential accident initiator. If the human error can only cause accidents that have already been considered in the licensing basis, then an accident of a different type has not been created.

Number and/or Type of Parameters Monitored

If an adverse impact resulted from the number and/or type of parameters monitored factor, there is no mechanism for a "number" or "type" of parameter to initiate an accident. Namely, the number of parameters monitored (e.g., 3, 4, 5, etc.) cannot, by itself, initiate an accident. Similarly, the type of parameters monitored (e.g., flow, level, pressure, voltage, etc.) cannot, by itself, initiate an accident. If an accident cannot be initiated, then it is impossible to initiate a new accident. If a new accident cannot be initiated, then a different accident cannot be created.

Information Presentation

If an adverse impact resulted from the information presentation factor, there is no mechanism for a "manner of presentation" to initiate an accident. If an accident cannot be initiated, then it is impossible to initiate a new accident. If a new accident cannot be initiated, then a different accident cannot be created.

4.5.2 Application of Guidance

From the main body of NEI 96-07, Section 4.3.5, the two considerations that need to be assessed when answering this question are credible and bounding. A *new* accident is not a *different* accident if the accident is determined to not be credible or, if credible, is bounded by an accident already considered in the UFSAR. Therefore, for the response to this Evaluation criterion to require submittal of a license amendment request for NRC review, the new accident must be both credible and not bounded.

For purposes of 50.59, a conclusion of *CCF Unlikely* is equivalent to a licensing condition of an accident initiator being NOT as likely to happen as those previously evaluated in the UFSAR (i.e., NOT credible). Without a credible accident initiator, a new accident cannot be created due to a CCF.

Alternately, a conclusion of *CCF Not Unlikely* is equivalent to a licensing condition of an accident initiator being as likely to happen as those previously evaluated in the UFSAR (i.e., credible). If an accident initiator is credible, then a new accident can be created. However, although a new accident may have been created, the determination of bounding needs to be addressed (using the generic guidance in the main body of NEI 96-07, Section 4.3.5).

Example 4-1. Application of "Credible" and "Bounding"

Currently, the only credible malfunction described in the UFSAR for an analog main feedwater control system is the loss of one main feedwater pump

(out of two pumps). A digital modification now controls both main feedwater pumps.

The conclusion of the CCF Susceptibility Analysis was *CCF not likely*, with the CCF causing the loss of both feedwater pumps. Thus, the credibility of a *new* accident has been established by the *CCF not likely* conclusion from the CCF Susceptibility Analysis.

To determine if the *new* accident (loss of both main feedwater pumps) is bounded by an accident already included in the UFSAR (loss of one main feedwater pump), the description and assumptions in the Loss of Feedwater accident need to be reviewed.

If the current accident analysis for the Loss of Feedwater accident conservatively considered the loss of both main feedwater pumps (even though only one pump could have failed originally), then it can be concluded that the new accident is *bounded* and does not create the possibility of an accident of a different type.

However, if the current accident analysis considered the loss of only one main feedwater pump, then an accident of a different type has been created because losing two pumps is different than losing one pump.

4.6 DOES THE ACTIVITY CREATE A POSSIBILITY FOR A MALFUNCTION OF AN SSC IMPORTANT TO SAFETY WITH A DIFFERENT RESULT?

Note: In the following discussions, the word "train" shall be assumed to include "channel" and "division," or any other designator used to describe redundant components and/or systems.

4.6.1 GENERAL CONSIDERATIONS

Level of Detail

The guidance is the same as that discussed in Section 4.2.1 above, or the main body of NEI 96-07, Sections 4.3.2 and 4.3.6.

Common Cause Failure Considerations

The guidance is the same as that discussed in Section 4.2.1 above.

HSI Considerations

Recalling the HSI factors that were addressed in the Screen that could lead to potential adverse impacts (i.e., physical interaction, the number and/or type of

parameters monitored, and information presentation), they may need to be considered here.

Physical Interaction

If an adverse impact resulted from the physical interaction with the digital system/component, human error would be the potential malfunction initiator. If the human error can only create results that have already been considered in the licensing basis, then a result of a different type has not been created.

Number and/or Type of Parameters Monitored

If an adverse impact resulted from the number and/or type of parameters monitored factor, there is no mechanism for a "number" or "type" of parameter to cause a result. Namely, the number of parameters monitored (e.g., 3 parameters, 4 parameters, etc.) cannot, by itself, cause a result. Similarly, the type of parameters monitored (e.g., flow, level, pressure, voltage, etc.) cannot, by itself, cause a result. However, the *use* or *application* of the number and/or type of parameters monitored could potentially create a different result.

Example 4-2. Number and/or Type of Parameters

Currently, the operator monitors only one parameter while filling a tank: wide-range level. When level reaches 95% ± 2%, the fill pump is manually stopped to prevent over-filling and/or over-pressurizing the tank. This process is described in exactly this detail in the UFSAR. To satisfy an accident analysis assumption (also described in the UFSAR), the tank must be filled to greater than or equal to 90% level. (All instrument uncertainties are accounted for in the accident analysis, so the indicated level may be used directly, without adjustment.) The result of the human error (i.e., over-filling and/or over-pressurizing the tank) is described in the UFSAR.

As part of a digital modification, both narrow-range and wide-range tank level indications will now be available.

A possible failure scenario involving the operator reading the wrong indication (i.e., narrow-range instead of wide-range) is postulated and determined to be credible, creating a new human error. This failure scenario involves reading the narrow-range indication instead of the wide-range indication and acting on the narrow-range indication value. This incorrect action causes the operator to stop the pump too soon. Stopping the pump too soon results in the tank potentially not being filled to the minimum expected volume assumed in an accident analysis described in the UFSAR.

To respond to this Evaluation criterion, the current *result* from a malfunction described in the UFSAR needs to be identified. In this case, the UFSAR describes the *result* as being the "over-filling and/or over-pressuring the tank."

With the new multiple level indications, a *result* involving "insufficient tank volume" is created. This *result* is different from the current *result*. Therefore, for this 10 CFR 50.59 Evaluation criterion, the response would be "YES" for the proposed activity of adding the narrow-range indication.

Information Presentation

If an adverse impact resulted from the information presentation factor, there is no mechanism for a "presentation method" to cause a result. Namely, the presentation method cannot, by itself, cause a result. However, the *use* or *application* of the presentation method could potentially create a different result.

Example 4-3. Information Presentation

Currently, the temperature indicator information necessary to correctly operate the facility is presented on the main control board using four redundant trains (A, B, C and D). Each train consists of a primary indication (identified as "1") and an alternate indication (identified as "2"), for a total of eight indications. These indications are used by the operators to identify a specific "undesirable plant condition" that requires the manipulation of plant equipment. The "undesirable plant condition" must be observed on 2-out-of-4 indicators (or 2-out-of-3 indicators if one channel is out-of-service) to be considered valid. For example, A1/B1 or B2/D2 would be valid comparisons. However, comparison of values across different indication types [i.e., primary-to-alternate (e.g., B1/B2 or C1/D2)] would NOT be considered a valid combination of indications (and is not allowed by procedure). This arrangement and process are described in exactly this detail in the UFSAR. Failure to identify the "undesirable plant condition" results in the plant equipment not being manipulated as assumed in an accident analysis described in the UFSAR. The result of this human error (i.e., plant equipment NOT being manipulated as required) is also described in the UFSAR.

As part of a digital modification, all of the analog indicators will be replaced with a touch screen that will have the capability to present three different displays: (1) each temperature reading individually [i.e., only one at a time (e.g., A2 or C1)], (2) by type of indication [i.e., either all four primary indications (A1, B1, C1 & D1) or all four alternate indications (A2, B2, C2 & D2)], and (3) both types of readings (i.e., primary and alternate) for a selected train (e.g., A1/A2, B1/B2, C1/C2 or D1/D2.).

Note that only the type display (of either type) satisfies the UFSAR description for being able to identify the "undesirable plant condition." None of the new displays perform any type of automatic indication comparison. The comparison is still performed manually by the operator.

A possible failure scenario involving the operator using an incorrect display screen (i.e., the train display instead of the type display) is postulated and determined to be credible, creating a new human error. [Note that an error involving the incorrect usage of the individual display instead of the type display is not credible since the display would contain only one value and would be intuitively obvious that a comparison cannot be performed with only one reading.] The human error will cause the operator to manipulate the plant equipment when it should not have been manipulated. Manipulating the plant equipment when it should not have been manipulated will create a new initiator of an accident that has already been evaluated in the UFSAR.

To respond to this Evaluation criterion, the current *result* from a malfunction described in the UFSAR needs to be identified. In this case, the UFSAR describes the *result* as being the "plant equipment not being manipulated as assumed in an accident analysis."

With the creation of new multiple display options, a *result* involving manipulation of equipment that should not have been manipulated is created. However, this is an "intermediate result," with the end result being that an accident (i.e., a specific plant-level response) will be initiated. Given that the initiated accident has already been evaluated in the UFSAR, this new *result* is **NOT** different from the current *result* . Therefore the response for this 10 CFR 50.59 Evaluation criterion would be "NO" for the proposed activity of adding the multiple displays.

Types of Malfunctions

Note that *new* malfunctions are not the issue when responding to this criterion. The main body of NEI 96-07, Section 4.3.6 states:

> "...a new failure mechanism is not a malfunction with a different result if the result or effect is the same as, or is bounded by, that previously evaluated in the UFSAR."

The key to assessing the proposed activity is to determine the set of failure mechanisms that are plausible at the appropriate level of detail and whether those failure mechanisms could prevent a design function from being performed as described in the UFSAR.

Results of the Hazard Analysis performed during the design effort should be used to identify the effects on the design function of failures that are as likely as those in the UFSAR.

The key issue is the effect of malfunctions (i.e., the *result*) due to failures of the digital device on the component and/or system in which it is installed. The Hazard Analysis will provide insights to component and/or system failures and their effects on SSCs. If failures of the digital device cause the component and/or system to malfunction (i.e., not perform its design function as described in the UFSAR), then the comparison needs to determine if the *result* of the component and/or system malfunction is bounded by, or different than, the *result* previously evaluated in the UFSAR.

Types of Results

Many types of *results* can be described in a UFSAR. In the main body of NEI 96-07, Section 4.3.6, the second bullet/example after the first paragraph states:

> "Provided the **end result** of the component or subsystem failure is the same as, or is bounded by, the results...described in the UFSAR..., then...[the activity]...would not create a 'malfunction with a different result'." [bold underline emphasis added]

In some cases, the *result* may be a transient or accident (i.e., a specific plant-level response) if the malfunction is a transient or accident initiator. In these cases, a discussion of the transient or accident that is initiated by the SSC malfunction will typically be described in the UFSAR in addition to the malfunction of the SSC itself and the physical result of the malfunctioning SSC. If a transient or accident is identified as a result of a malfunction, the plant-level response described in the transient or accident would be considered the **end result**.

For activities involving digital modifications, only the **end result** will be the *result* of interest. For clarity, all results other than the **end result** will be classified as "intermediate results." No "intermediate results" need to be considered if more than one level of result is described.

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

- Component Level Result
- System Level Result (from the component level malfunction and result)

- Plant Level Result/Response (from the system level malfunction and result). [These results would typically include the physical effects (e.g., maximum RCS pressure), the type of event (e.g., increase/decrease in heat removal) and/or radiological dose.]

In this case, the Component Level and System Level results would be considered "intermediate results" and the Plant Level Result/Response would be considered the **end result**.

Therefore, if a transient or accident is identified as a result of a malfunction, the initiation of a different transient or accident than that which is already described in the UFSAR is not a different result *provided that the plant-level response is bounded by another transient or accident.*

Example 4-4. Types of Results

A credible malfunction described in the UFSAR for an analog main feedwater control system involves the loss of one main feedwater pump (out of two pumps). A digital modification now controls both main feedwater pumps and is found to be susceptible to a CCF that causes the loss of both main feedwater pumps.

Currently, the UFSAR describes this malfunction of one main feedwater pump as resulting in a reduction in flow (intermediate result #1) to the steam generators, which initiates the Loss of Feedwater accident (intermediate result #2). For the Loss of Feedwater accident, the UFSAR identifies peak Reactor Coolant System (RCS) pressure as the key numerical analysis result (end result).

The credibility of a new malfunction initiator has been established by identification of the CCF so an examination of the results currently described in the UFSAR needs to be performed.

The loss of both main feedwater pumps causes no flow to the steam generators ("new" intermediate result #1), which initiates a Loss of Feedwater accident ("new" intermediate result #2) and affects the numerical result of the accident analysis ("new" **end result**).

Although the impact on intermediate result #1 (magnitude of the flow decrease) is more severe (i.e., from a *reduction* to *none*), it is not the result that determines the response to this Evaluation criterion. Even though the impact on intermediate result #2 is the same, it also is not the result that determines the response to this Evaluation criterion.

Verifying that the calculated value of maximum RCS pressure continues to meet its applicable acceptance criteria (i.e., the maximum RCS pressure, a specific plant-level response) would allow the malfunction **end result** to be considered NOT different and a "NO" response to this Evaluation criterion would be established.

Other Factors to Consider

The following considerations may be helpful when developing the response to this Evaluation criterion:

- Does the modified system have the same failure mode on loss of power as the system being replaced? If the failure mode is different, are the results bounded by what was evaluated previously in the UFSAR?

- Is the response of the modified system on restoration of power different from that of the system being replaced? If so, are the results bounded by what was evaluated previously in the UFSAR?

- Does the system or equipment reset to operating parameters and settings established for the specific system, or does it go to a default set of parameters when the system is reset? If the system is reset to a default set of parameters, what effect do they have on plant operation? Are the results bounded by what was evaluated previously in the UFSAR?

- Does the human-system interface introduce failure modes different from those of the existing system? If so, are the results bounded by what was evaluated previously in the UFSAR?

- Have assessments of system-level failure modes and effects for the new system or equipment identified any new types of system-level failures (that are as likely to occur as those failures previously considered in the UFSAR) that would not be bounded by the results previously considered in the UFSAR?

- Does the architecture of the system exhibit a single failure that results in more severe consequential effects (e.g., reduced segmentation due to combining previously separate functions, several input channels sharing an input board, central loop processor for many channels)?

4.6.2 APPLICATION OF GUIDANCE

From the main body of NEI 96-07, Section 4.3.6, the two considerations that need to be assessed when answering this question are as likely to happen as those described in the UFSAR (i.e., credible) and bounding.

For purposes of 50.59, a conclusion of *CCF Unlikely* is equivalent to a licensing condition of a CCF malfunction not being as likely to happen as those described in the UFSAR (i.e., not credible). If a malfunction due to a CCF is not credible, then the malfunction does not need to be considered when assessing the type of result produced.

Alternately, for purposes of 50.59, a conclusion of *CCF Not Unlikely* is equivalent to a licensing condition of a CCF malfunction as likely to happen as those malfunctions described in the UFSAR (i.e., credible). If a malfunction due to a CCF is credible, then the malfunction needs to be considered when assessing if the results from the CCF are bounded by the results previously evaluated in the UFSAR.

4.7 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 criterion 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 the main body of NEI 96-07, Section 4.3.7 applies.

4.8 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 the main body of NEI 96-07, Section 4.3.8 applies.

5 EXAMPLES

5.1 INTRODUCTION

Scope

In general, the examples provided below illustrate the application of the above guidance for **only** the digital portion of the facility modification.

Typically, digital modifications also involve impacts to non-digital aspects of the facility and/or procedures. These non-digital aspects are not illustrated in the examples because they are not unique to digital modifications. The absence of these non-digital aspects in the examples does not imply that they are not important or that they do not need to be addressed. On the contrary, these non-digital aspects are just as important as the aspects directly associated with the digital portion of the modification itself.

Screen Portion of the Examples

Typical digital modifications can also involve impacts to non-digital aspects of the facility and their UFSAR-described design functions. For the "facility," electrical loading, seismic considerations, EMI, heat loads, and environmental qualification may need to be considered. For "procedures," actions taken, operator response times and the fundamental means of how a design function is performed or controlled may need to be considered.

The Screen examples do not illustrate the full Screen development process. For example, the process for identifying the pertinent SSCs and their pertinent UFSAR-described design functions is not illustrated. However, these activities within the Screen process are no different for digital modifications than for non-digital modifications.

Responses for only Screen Considerations 1 and 2 are provided to illustrate specific application of the digital-guidance in Section 3 above. Responses for the Method of Evaluation consideration and the Test/Experiment consideration are not provided since the processes for developing these responses are no different for digital modifications than for non-digital modifications.

Evaluation Portion of the Examples

The Evaluation examples do not illustrate the full Evaluation development process. For example, the processes for identifying the pertinent accidents,

accident initiators, malfunctions, malfunction initiators, radiological dose analyses (including their inputs and assumptions) and determining the appropriate level of detail described in the UFSAR for these considerations are not illustrated. However, these activities within the Evaluation process are no different for digital modifications than for non-digital modifications.

In general, responses for only Evaluation Criteria 2, 5 and 6 are provided to illustrate specific application of the digital-guidance in Section 4 above. In Example 6 only, a response for Evaluation Criterion 1 is provided because the digital modification involves a unique aspect for which illustration will benefit the user.

5.2 EXAMPLE 1 - ADDITION OF A SINGLE DIGITAL CONTROL SYSTEM

PURPOSE AND SUMMARY

The purpose of this example is to illustrate the replacement of analog control functions with a digital control system for non-safety-related SSCs for which CCF is not a concern (i.e., for a single application of a digital control system). No HSI modifications are involved.

The Screen conclusion was *not adverse* for the digital-related impacts.

SCREEN

Title:

Replacement of Gaseous Radwaste System Analog Controls with a Digital Control System

Proposed Activity Description:

Install a digital control system to replace the analog control functions for the processing of waste gas.

Design Function Identification:

The UFSAR-described design function of the radioactive Waste Gas System and the Waste Gas Decay Tank is to store radioactive waste gases until they decay sufficiently to be released to the environment.

Screen Responses:

1. **Does the proposed activity involve a modification, addition to, or removal of a SSC such that the design function of the SSC, as described in the UFSAR, is adversely affected?**

   NO.

Combination of Components/Functions Assessment

Most of the current functions within the Waste Gas System (with the exception of the manual termination of compressor operation) will be combined into one digital control system. Although the combination of functions into one digital device reduces the separation of individual controls, the combination does not affect the variety and/or layers of design described

in the UFSAR. Furthermore, there was no reduction in the reliability of performing a design function because no new malfunctions or accident initiators were created. Therefore, there is *no adverse* impact on the UFSAR-described design function of the radioactive Waste Gas System or the Waste Gas Decay Tank to store gas due to combination-related issues.

Dependability Assessment

To address the dependability of the new digital control system, a review of the available operating history of the hardware and software was performed and documented. No examples of unexplained failures or behaviors were identified.

Design measures (including data validation and cyclic software architecture) were implemented to maintain or improve the dependability of the new digital control system relative to the previously installed analog system.

The software was developed and tested using a software requirements specification, factory acceptance testing, a site acceptance testing plan, Failure Modes and Effects Analysis (FMEA), and a verification and validation plan. The software will be controlled by the appropriate site configuration management procedures and equipment operating instructions.

Therefore, since the dependability of the digital control system has been established, the dependability of the associated design functions has been confirmed.

There is *no adverse* impact on a design function due to a reduction in the reliability of performing a design function.

2. Does the proposed activity involve a change to a procedure that adversely affects how UFSAR described SSC design functions are performed or controlled?

NO.

No portion of the proposed activity involves how individuals interact with the new digital devices or the information presented by the new devices. The same information will be available with the new devices and the information will be used in the same manner. Since no HSI aspects are included in this change, *no adverse* impacts are possible.

EVALUATION: Not required.

5.3 EXAMPLE 2 - REPLACEMENT OF REDUNDANT COMPONENTS

PURPOSE AND SUMMARY

The purpose of this example is to illustrate the replacement of redundant safety-related analog recorders with digital recorders that contain the same software and CCF is a concern. No HSI modifications are involved.

The Screen conclusion was *adverse* due to a digital-related impact.

In the Evaluation, a hardware-related CCF conclusion of *unlikely* and a software-related CCF conclusion of *not unlikely* were used from the technical support work. The Evaluation concluded that a License Amendment Request for the digital-related impacts was NOT required.

SCREEN

Title:

Replacement of Post-Accident Monitoring System (PAMS) Analog Recorders with Digital Recorders

Proposed Activity Description:

The proposed activity involves an analog-to-digital upgrade of two redundant PAMS recorders. The new recorders in each division are identical, and each recorder is configured for displaying and trending two reactor vessel parameters: reactor pressure (RP) and wide range water level (WRWL).

Design Function Identification:

The UFSAR describes RP and WRWL recorders as redundant, electrically independent, and operable during and after a Loss of Coolant Accident (LOCA). The UFSAR describes these recorders as part of the redundant instrumentation that are credited for providing RG 1.97 indication for plant specific Type A variables.

Screen Responses:

1. **Does the proposed activity involve a modification, addition to, or removal of a SSC such that the design function of the SSC, as described in the UFSAR, is adversely affected?**

   YES.

Combination of Components/Functions Assessment

The proposed activity does not involve the combination of components or functions, so there is *no adverse* impact on a design function due to combination-related issues.

Since identical software will be used in each recorder, there is an ***adverse*** impact on the independence of the PAMS recorders described in the UFSAR.

Dependability Assessment

Since the new digital recorders perform the exact same functions as the original analog recorders, a direct correlation can be made by comparing the dependability of each device.

A commercial grade dedication (CGD) of the digital equipment was performed. The CGD demonstrated the digital equipment was equivalent to equipment developed under a 10 CFR 50, Appendix B QA program using a documented life-cycle process.

Based on the qualification activities and critical digital review documented in the CGD report, including software verification and validation, applicable operating history survey, the digital equipment is considered a highly reliable system on a level equal to, or exceeding, the analog equipment.

There is *no adverse* impact on a design function due to a reduction in the reliability of performing a design function.

2. Does the proposed activity involve a change to a procedure that adversely affects how UFSAR described SSC design functions are performed or controlled?

NO.

No portion of the proposed activity involves how individuals interact with the new digital devices or the information presented by the new devices. The same information will be available with the new devices and the information will be used in the same manner. Since no HSI aspects are included in this change, *no adverse* impacts are possible.

EVALUATION

Criterion 2: Does the proposed activity result in more than a minimal increase in the likelihood of occurrence of

a malfunction of an SSC important to safety previously evaluated in the UFSAR?

NO.

Level of Detail

The UFSAR describes the PAMS recorders as independent and redundant two-pen recorders that provide indication to the operators to be used for planned manual actions are assumed in accidents for the long-term core cooling following the initial automatic system initiation and long-term decay heat removal. Two redundant PAMS recorders are required to ensure that no single failure can mislead the operator and prevent bringing the plant to a safe condition following an accident. Therefore, the PAMS recorders are explicitly described and will be the appropriate level for which potential impacts on malfunction likelihood will be addressed.

The malfunction described in the UFSAR would be the loss of indication or ambiguous indication to the plant operators.

CCF Considerations - Hardware

The PAMS recorders have been analyzed to perform properly within the Main Control Board environment during normal and accident conditions. Each recorder is separated and isolated (physically and electrically) further reducing the vulnerability of a CCF due to environmental factors.

Based on this assessment, it can be concluded that a hardware-related CCF is *unlikely*.

CCF Considerations - Software

CGD of the software was performed to establish software quality and signify that the likelihood of a software defect is low. A critical digital review was performed, including an independent review of the PAMS recorder software design and configuration process. The CGD process, which included the independent software review, demonstrated the PAMS recorder software is equivalent to software developed under an Appendix B Quality Assurance Program. The recorder's application-specific configuration was performed using the site's Software Quality Assurance processes for safety-related digital devices. Although the recorder was commercial grade dedicated in accordance with accepted industry practices, there is no evidence of testing all internal and external state combinations. Additionally, there is a lack of

substantial recorder operating history with new firmware installed on the device.

Based on this assessment, it is concluded that a software-related CCF is *not unlikely*.

[*Author's Note: If all internal and external state combinations had been tested OR if there was evidence of substantial operating history with the new firmware, a software-related CCF of unlikely would have been concluded.*]

Justifications and Conclusions

The determination that a hardware-related CCF is *unlikely* is equivalent to a licensing condition of a malfunction that is NOT credible. Therefore, without a credible new malfunction initiator due to the hardware, there is not more than a minimal increase in the likelihood of a malfunction of an SSC important to safety previously evaluated in the UFSAR due to a hardware-related CCF.

The determination that a software-related CCF is *not unlikely* is equivalent to a licensing condition of a malfunction that IS credible. However, because the software was developed in accordance with a defined process, an increase in the likelihood of a malfunction previously evaluated in the UFSAR is not discernible (but is attributable to the proposed activity).

Therefore, since an increase in the likelihood of a malfunction is not discernible, there is not more than a minimal increase in the likelihood of a malfunction of an SSC important to safety previously evaluated in the UFSAR due to a software-related CCF.

Criterion 5: Does the proposed activity create a possibility for an accident of a different type than previously evaluated in the UFSAR?
NO.

The determination that a hardware-related CCF is *unlikely* is equivalent to a licensing condition of an accident initiator that is NOT credible. Without a credible new accident initiator, a new accident cannot be created due to a hardware-related CCF. Therefore, since a new accident cannot be created, it is not possible to create an accident of a different type than previously evaluated in the USFAR due to a hardware-related CCF.

The determination that a software-related CCF is *not unlikely* is equivalent to a licensing condition of an accident initiator that IS credible. However, the

PAMS recorders are utilized in the monitoring and initiation of manual actions post-accident, and is not an initiator of any accident analyzed in the UFSAR. Furthermore, the proposed activity does not create a credible scenario in which the PAMS recorder could become an accident initiator.

Therefore, without a credible scenario in which the new accident initiator would apply, it is not possible to create an accident of a different type than previously evaluated in the USFAR due to a software-related CCF.

Criterion 6: **Does the proposed activity create a possibility for a malfunction of an SSC important to safety with a different result than any previously evaluated in the UFSAR?**

NO.

Level of Detail

Same level as determined in the response to Criterion #2.

CCF Considerations - Hardware

Based on the assessment outlined in the response to Criterion #2, it was concluded that a hardware-related CCF was *unlikely*.

CCF Considerations - Software

Based on this assessment outlined in the response to Criterion #2, it was concluded that a software-related CCF was *not unlikely*.

Results Assessment

Previously Evaluated Results:

The UFSAR describes the failure of the PAMS recorders as causing improper manual operator actions or inability of the operator to properly evaluate automatic responses and adequate core cooling using RPV pressure and level indication provided by the recorders.

New Results:

With failure of both PAMS recorders due to CCF, the operators could defeat a required safety function or fail to accomplish a required safety function.

Comparison of Results:

The new results are the same as the results previously evaluated in the UFSAR.

Justifications and Conclusions

The determination that a hardware-related CCF is *unlikely* is equivalent to a licensing condition of a CCF malfunction that is NOT credible. Since a malfunction due to a hardware CCF is not credible, no results different from those previously evaluated in the UFSAR are possible.

The determination that a software-related CCF is *not unlikely* is equivalent to a licensing condition of a CCF malfunction that IS as credible as those malfunctions described in the UFSAR. The PAMS recorders malfunction results are bounded by the malfunction results previously evaluated in the UFSAR.

Thus, this activity will not create the possibility for a malfunction with a different result than any previously evaluated in the UFSAR.

5.4 EXAMPLE 3 - REPLACEMENT OF REDUNDANT CONTROL DEVICES

PURPOSE AND SUMMARY

The purpose of this example is to illustrate the replacement of analog control devices on redundant safety-related SSCs with digital control devices that contain the same software and CCF is a concern. No HSI modifications are involved.

The Screen conclusion was *adverse* due to the digital-related impacts.

In the Evaluation, a hardware-related CCF conclusion of *unlikely* and a software-related CCF conclusion of *not unlikely* were used from the technical support work. The Evaluation concluded that a License Amendment Request for the digital-related impacts was NOT required.

SCREEN

Title:

Replacement of Analog Motor-Operated Potentiometer (MOP) with a Digital Reference Adjuster (DRA)

Proposed Activity Description:

The proposed activity will replace the existing emergency diesel generator (EDG) excitation system MOP with a DRA.

Design Function Identification:

The UFSAR describes the standby alternating current power supply and distribution system, which includes two completely independent EDG systems per nuclear unit.

Screen Responses:

1. Does the proposed activity involve a modification, addition to, or removal of a SSC such that the design function of the SSC, as described in the UFSAR, is adversely affected?

YES.

Combination of Components/Functions Assessment

The proposed activity does not involve the combination of components or functions, so there is *no adverse* impact on a design function due to combination-related issues.

Since identical software will be used in each DRA, there is an ***adverse*** impact on the independence of the EDGs described in the UFSAR.

Dependability Assessment

Since the DRA performs the exact same function as the MOP, a direct correlation can be made by comparing the dependability of each device.

A commercial grade dedication (CGD) of the digital equipment was performed. The CGD demonstrated the digital equipment was equivalent to equipment developed under a 10 CFR 50, Appendix B QA program using a documented life-cycle process.

Based on the qualification activities and critical digital review documented in the CGD report, including software verification and validation, applicable operating history survey, the digital equipment is considered a highly reliable system on a level equal to, or exceeding, the analog equipment.

There is *no adverse* impact on a design function due to a reduction in the reliability of performing a design function.

2. Does the proposed activity involve a change to a procedure that adversely affects how UFSAR described SSC design functions are performed or controlled?

NO.

No portion of the proposed activity involves how individuals interact with the new digital devices or the information presented by the new devices. The same information will be available with the new devices and the information will be used in the same manner. Since no HSI aspects are included in this change, *no adverse* impacts are possible.

EVALUATION

Criterion 2: Does the proposed activity result in more than a minimal increase in the likelihood of occurrence of a malfunction of an SSC important to safety previously evaluated in the UFSAR?

NO.

Level of Detail

The MOP is not explicitly described in the UFSAR, but is part of the EDG system. Therefore, the EDG system will be the appropriate level for which impacts on malfunction likelihood will be addressed.

The only pertinent malfunction previously evaluated in the UFSAR is a single failure (i.e., the loss of one EDG out of two).

CCF Considerations - Hardware

The DRA has been analyzed to perform properly within the EDG environment during normal and accident conditions. The DRA will be installed in all four EDG voltage regulator excitation systems. Each EDG is separated and isolated (physically and electrically) further reducing the vulnerability of a common cause failure (CCF) due to environmental factors.

Based on this assessment, it can be concluded that a hardware-related CCF is *unlikely*.

CCF Considerations - Software

CGD of the software was performed to establish software quality and signify that the likelihood of a software defect is low. A critical digital review was performed, including an independent review of the software design and configuration process. The CGD process, which included the independent software review, demonstrated the software is equivalent to software developed under an Appendix B Quality Assurance Program. The device's application-specific configuration was performed using the site's Software Quality Assurance processes for safety-related digital devices. Although the DRA received some testing during the CGD process, there is no evidence of extensive testing of all internal and external state combinations, and there is no analysis that demonstrates untested state combinations are irrelevant.

Based on this assessment, it is concluded that a software-related CCF is *not unlikely*.

[*Author's Note: If all internal and external state combinations had been tested, a software-related CCF of unlikely would have been concluded.*]

Justifications and Conclusions

The determination that a hardware-related CCF is *unlikely* is equivalent to a licensing condition of a malfunction that is NOT credible. Therefore, without a credible new malfunction initiator due to the hardware, there is not more than a minimal increase in the likelihood of a malfunction of an SSC important to safety previously evaluated in the UFSAR due to a hardware-related CCF.

The determination that a software-related CCF is *not unlikely* is equivalent to a licensing condition of a malfunction that IS credible. However, because the software was developed in accordance with a defined process, and complies with the applicable industry standards and regulatory guidance, an increase in the likelihood of a malfunction previously evaluated in the UFSAR is not discernible (but is attributable to the proposed activity).

Therefore, since an increase in the likelihood of a malfunction is not discernible, there is not more than a minimal increase in the likelihood of a malfunction of an SSC important to safety previously evaluated in the UFSAR due to a software-related CCF.

Criterion 5: Does the proposed activity create a possibility for an accident of a different type than previously evaluated in the UFSAR?

NO.

The determination that a hardware-related CCF is *unlikely* is equivalent to a licensing condition of an accident initiator that is NOT credible. Without a credible new accident initiator, a new accident cannot be created due to a hardware-related CCF. Therefore, since a new accident cannot be created, it is not possible to create an accident of a different type than previously evaluated in the USFAR due to a hardware-related CCF.

The determination that a software-related CCF is *not unlikely* is equivalent to a licensing condition of an accident initiator that IS credible. However, the EDG system is utilized in the mitigation of accidents and is not an initiator of any accident analyzed in the UFSAR. Furthermore, the proposed activity does not create a credible scenario in which the EDG system could become an accident initiator

Therefore, without a credible scenario in which the new accident initiator would apply, it is not possible to create an accident of a different type than previously evaluated in the USFAR due to a software-related CCF.

Criterion 6: **Does the proposed activity create a possibility for a malfunction of an SSC important to safety with a different result than any previously evaluated in the UFSAR?**

NO.

Level of Detail

Same level as determined in the response to Criterion #2.

CCF Considerations - Hardware

Based on the assessment outlined in the response to Criterion #2, it was concluded that a hardware-related CCF was *unlikely*.

CCF Considerations - Software

Based on the assessment outlined in the response to Criterion #2, it was concluded that a software-related CCF was *not unlikely*.

Results Assessment

Previously Evaluated Result:

The only pertinent result described in the UFSAR due to a malfunction is that one EDG (out of two) will be available.

New Result:

For any reason (including a software-related CCF), if the DRA is "parked" at the correct resistance value (for 4160 V control) and an EDG is started (manually or automatically), the DRA will stay "parked" at the 4160 V setting. Only on a manual start (non-emergency) does the operator have the ability to vary the output voltage by varying the output resistance of the DRA. In either condition (emergency or non-emergency), at least one EDG will be available.

The DRA cannot prevent an EDG from starting and producing an output voltage. Failure of the DRA would manifest itself by producing a voltage in the range of 3750 V to 4600 V (i.e., at a value other than the 4160 V safety bus voltage). The Technical Specifications require the EDG voltage to be $\geq$3750 V and $\leq$4300 V. If the DRA caused the safety bus voltage to be >4300 VAC and $\leq$4600 VAC, this condition would be noticed by the control room

operator (and is annunciated by an alarm) and action could be taken to reduce the voltage. This set of conditions and results is no different with the DRA than with the MOP.

While the EDG is on standby (shutdown and unloaded, awaiting a start signal), the DRA continuously provides a pre-set resistance value to the EDG voltage regulator corresponding to the required safety bus voltage (i.e., 4160 VAC). The DRA is designed such that a "freeze" or an "unintended operation" of the executable code will lock the DRA output resistance at the safety bus voltage setpoint (4160 VAC). There is no credible disturbance (external or internal) that causes the executable code to arbitrarily or randomly change the DRA output resistance setpoint from the 4160 VAC value. Therefore, at least one EDG will be available.

Comparison of Results:

All of the new results are the same as the results previously evaluated in the UFSAR.

Justifications and Conclusions

The determination that a hardware-related CCF is *unlikely* is equivalent to a licensing condition of a CCF malfunction that is NOT credible. Since a malfunction due to a hardware-related CCF is not credible, no results different from those previously evaluated in the UFSAR are possible.

The determination that a software-related CCF is *not unlikely* is equivalent to a licensing condition of a CCF malfunction that is as credible as those malfunctions described in the UFSAR.

The DRA failure modes are bounded by the failure modes of the MOP and the result is the same at the EDG system level (i.e., at least one EDG will be available). The result of DRA failure is bounded by the result currently described in the UFSAR (i.e., at least one EDG will be available following any malfunction).

Therefore, the results are not different from those previously evaluated in the UFSAR.

5.5 EXAMPLE 4 - REPLACEMENT OF REDUNDANT CONTROL SYSTEMS

PURPOSE AND SUMMARY

The purpose of this example is to illustrate the replacement of analog control systems on redundant safety-related SSCs with digital control systems that contain the same software and CCF is a concern. No HSI modifications are involved.

The Screen conclusion was *adverse* due to the digital-related impacts.

In the Evaluation, a hardware-related CCF conclusion of *unlikely* and a software-related CCF conclusion of *unlikely* were used from the technical support work. The Evaluation concluded that a License Amendment Request for the digital-related impacts was NOT required.

SCREEN

Title:

Replacement of Chiller Analog Control Systems with Digital Control Systems

Proposed Activity Description:

1. The proposed activity will replace the two existing main control room (MCR) Train A and B chillers analog control systems (one per train) with two commercial off-the-shelf digital control systems (one per train).

2. The proposed activity involves the combination of existing electrical and mechanical components (i.e., controllers, bistables, timers, etc.) and functions (i.e., relay logic, equipment protective trips, alarms, etc.) within each division, but the separation and independence of each division is maintained.

[*Author's Note: To illustrate how activities other than those directly related to the harware, software or HSI aspects can accompany a digital modification, all of the activities identified in #3 below are also part of the overall modification. However, these activities are not unique to "digital" since all of these additional activities could have been implemented with a non-digital modification. None of these activities will be addressed in this example, which focuses only on the strictly digital aspects of the modification. In an actual Screen, all of these additional actvities would need to be addressed.*]

3. Several functional performance and sequence of operation changes for the MCR chillers will be made to increase the reliability of the new chillers. These changes include:

(a) The existing system requires manually resetting the controls to energize the high temperature trip relay when electrical power is lost for greater than 60 seconds. With the new system, this manual action is no longer required.

(b) The existing control logic could allow the chiller to start without chilled water flow being present, potentially freezing the chiller, if the chilled water pump shaft was decoupled from its motor. The new control system's start logic will not allow the chiller to start or run when chilled water flow is not present.

(c) The exisiting controller starts the compressor immediately when needed. The new controller will postpone starting the compressor for a 15 second time period while it monitors the power supply to determine that the power supply is stable.

(d) The new control system contains a new feature that will allow the chiller to operate in a limited condition when certain process values enter off-normal conditions.

(e) The new control system contains a new feature that calculates the anticycle time based on how long the chiller was running prior to stopping and how long the chiller has been stopped.

Design Function Identification:

Design Functions for Activity #1:

The UFSAR states that plant locations containing safety-related equipment that need a controlled environment to perform required accident mitigation operations are served by fully redundant environmental control systems.

The UFSAR describes the MCR air conditioning system as consisting of two 100% capacity units, with each unit meeting the single failure criterion, comprised of two 100% capacity package water chillers, two 100% capacity fan-coil type air handling units, and associated pumps, piping, ductwork, and controls.

Design Functions for Activity #2:

The UFSAR states that the MCR air conditioning system is designed "to maintain temperature and humidity conditions throughout the building for the protection, operation, and maintenance and testing of plant controls, and for the safe, uninterrupted occupancy of the main control room (MCR) habitability system (MCRHS) area during an accident and the subsequent recovery period" and the MCR air conditioning system consists of "two 100% capacity units. Each meets the single failure criterion...."

Screen Responses:

1. **Does the proposed activity involve a modification, addition to, or removal of a SSC such that the design function of the SSC, as described in the UFSAR, is adversely affected?**

   YES.

Combination of Components/Functions Assessment

For activity #1, since identical software will be used in each digital control system, there is an ***adverse*** impact on the independence of the chillers described in the UFSAR.

For activity #2, combining components and functions is *not adverse* because the consolidation is implemented only within each independent division; thereby continuing to meet single failure criteria as described in the UFSAR and not creating any new failure mechanisms.

Dependability Assessment

Since the digital control system performs the exact same functions as the analog control system, a direct correlation can be made by comparing the dependability of each control system.

A commercial grade dedication (CGD) of the digital equipment was performed. The CGD demonstrated the digital equipment was equivalent to equipment developed under a 10 CFR 50, Appendix B QA program using a documented life-cycle process.

Based on the qualification activities and critical digital review documented in the CGD report, including software verification and validation, applicable operating history survey, the digital equipment is considered a highly reliable system on a level equal to, or exceeding, the analog equipment.

There is *no adverse* impact on a design function due to a reduction in the reliability of performing a design function.

2. Does the proposed activity involve a change to a procedure that adversely affects how UFSAR described SSC design functions are performed or controlled?

NO.

No portion of the proposed activity involves how individuals interact with the new digital devices or the information presented by the new devices. The same information will be available with the new devices and the information will be used in the same manner. Since no HSI aspects are included in this change, *no adverse* impacts are possible.

EVALUATION

Criterion 2: Does the proposed activity result in more than a minimal increase in the likelihood of occurrence of a malfunction of an SSC important to safety previously evaluated in the UFSAR?

NO.

Level of Detail

The control systems for the MCR chillers are not explicitly described in the UFSAR, but are part of the chiller system. Therefore, the chiller system will be the appropriate level for which impacts on malfunction likelihood will be addressed.

As described in the UFSAR, two malfunctions of the MCR chillers are described: (1) failing to start, and (2) stops, both of which are caused by mechanical or electrical failures.

The initiators of the existing credible malfunctions identified in the UFSAR for each MCR chiller are:

1. Electrical Failures

2. Mechanical Failures.

Hazard Analysis

The FMEA did not identify any single failure modes of the digital control system that would result in loss of safety function of the associated air-conditioning system.

CCF Considerations - Hardware

The environment in which the digital control system will operate (EMI/RFI susceptibility, seismic, temperature, humidity, and radiological) has been evaluated, further reducing the vulnerability of a CCF due to environmental factors.

A third-party dedicator evaluated the hardware design development process used by the commercial vendor and reviewed the digital control system for potential hazards and failure modes with regard to hardware. The review process, results, and conclusions are contained in the Critical Digital Review (CDR) and FMEA. The evaluation in the CDR also included an operating history review of control system users with similar applications that the users viewed as operationally critical to their plants' performance.

Based on this assessment, it can be concluded that a hardware-related CCF is *unlikely*.

CCF Considerations - Software

A third-party dedicator evaluated the software development process used by the commercial vendor, performed software code reviews, performed verification and validation (V&V) activities to verify all control systems requirements in a similar configuration to the existing plant's installation, and reviewed the digital control system for potential hazards and failure modes with regard to software.

The review process, results, and conclusions are contained in the CDR, Software Requirements Specification (SRS), Software Design Document (SDD), Software Verification and Validation Report (SVVR), Hazards Analysis, and FMEA. The third-party dedicator concluded that the likelihood of software failure is low enough to be considered acceptable. Successful Factory Acceptance Testing operated the chiller package utilizing MCR chiller specific firmware and software which further supports the conclusions reached by the third party dedicator.

100% of the digital control system's software was reviewed and evaluated. In each instance, the code was compliant or the deviation did not warrant a

modification to the code and was not classified as an issue. All identified issues were resolved.

Extensive validation testing, developed from the code review and based upon the documented SRS, was performed by utilizing a test bed with hardware, base software, and specific application configuration settings. The validation testing demonstrated that the digital control system (hardware and software) performed as specified in the SRS under normal and abnormal conditions.

The CCF Susceptibility Analysis determined that most sources of CCF were unlikely, with the exception of a CCF due to a single design defect, for which sufficient preventive measures for the controller operating system could not be fully demonstrated. However, other limiting and mitigative measures are in place to drive the likelihood of CCF from a design defect much lower than those failures already considered in the licensing basis.

Based on this assessment, it is concluded that a software-related CCF is *unlikely*.

Justifications and Conclusions

The determination that a hardware-related CCF is *unlikely* is equivalent to a licensing condition of a CCF malfunction that is NOT credible. Therefore, without a credible new malfunction initiator due to the hardware, there is not more than a minimal increase in the likelihood of a malfunction of an SSC important to safety previously evaluated in the UFSAR due to a hardware-related CCF.

The determination that a software-related CCF is *unlikely* is equivalent to a licensing condition of a CCF malfunction that is NOT credible. Without a credible new malfunction initiator due to the software, a malfunction due to a software CCF is not credible. Therefore, there is not more than a minimal increase in the likelihood of a malfunction of an SSC important to safety previously evaluated in the UFSAR due to a software-related CCF.

Criterion 5: Does the proposed activity create a possibility for an accident of a different type than previously evaluated in the UFSAR?

NO.

The determination that a hardware-related CCF is *unlikely* is equivalent to a licensing condition of an accident initiator that is NOT credible. Without a credible new accident initiator, a new accident cannot be created due to a

hardware-related CCF. Therefore, since a new accident cannot be created, it is not possible to create an accident of a different type than previously evaluated in the USFAR due to a hardware-related CCF.

The determination that a software-related CCF is *unlikely* is equivalent to a licensing condition of an accident initiator that is NOT credible. Furthermore, a MCR chiller is a support system utilized in the mitigation of accidents and is not an initiator of any accident analyzed in the UFSAR and the proposed activity does not create a credible scenario in which the MCR chiller system could become an accident initiator.

Therefore, without a credible scenario in which the new accident initiator would apply, it is not possible to create an accident of a different type than previously evaluated in the USFAR due to a software-related CCF.

Criterion 6: **Does the proposed activity create a possibility for a malfunction of an SSC important to safety with a different result than any previously evaluated in the UFSAR?**

NO.

Level of Detail

Same level as determined in the response to Criterion #2.

CCF Considerations - Hardware

Based on the assessment outlined in the response to Criterion #2, it was concluded that a hardware-related CCF was *unlikely*.

CCF Considerations - Software

Based on the assessment outlined in the response to Criterion #2, it was concluded that a software-related CCF was *unlikely*.

Result

The UFSAR states that the failure of only one of the redundant chillers is possible and that the standby chiller will start.

Justifications and Conclusions

The determination that a hardware-related CCF is *unlikely* is equivalent to a licensing condition of a CCF malfunction that is NOT credible. Since a malfunction due to a hardware-related CCF is not credible, no results different from those previously evaluated in the UFSAR are possible.

The determination that a software-related CCF is *unlikely* is equivalent to a licensing condition of a CCF malfunction that is NOT credible. Since a malfunction due to a software-related CCF is not credible, no results different from those previously evaluated in the UFSAR are possible.

5.6 EXAMPLE 5 - REPLACEMENT OF REDUNDANT CONTROL SYSTEMS

PURPOSE AND SUMMARY

The purpose of this example is to illustrate the replacement of analog control systems on redundant safety-related SSCs with digital control systems that contain the same software and CCF is a concern. No HSI modifications are involved.

The Screen conclusion was *adverse* due to the digital-related impacts.

In the Evaluation, a hardware-related CCF conclusion of *unlikely* and a software-related CCF conclusion of *not unlikely* were used from the technical support work. The Evaluation concluded that a License Amendment Request for the digital-related impacts was NOT required.

As part of this example, a portion of the response to Criterion #6 will be modified to "fabricate" an Evaluation conclusion that a License Amendment Request for the digital-related impacts IS required. This "fabricated" conclusion will be clearly indicated at the end of the response to Criterion #6 as "ALTERNATE Justifications and Conclusions for a Software-Related CCF."

SCREEN

Title:

Replacement of Emergency Diesel Generator (EDG) Voltage Regulator/Exciter Analog Control System with a Digital Control System

Proposed Activity Description:

This proposed activity involves replacement of the voltage regulator/exciter analog control system on each EDG with a digital control system. The digital control system uses proprietary equipment and software that is programmable.

The principal digital component is the programmable Automatic Voltage Regulator (AVR). Other components of this digital control system are:

(1) Control Board which contains the control functions and fault diagnostics.

(2) Operator control panel displays (i.e., a new human system interface).

(3) Technology Board which implements the software for open-loop and closed-loop control.

(4) Serial communications unit which consists of a Serial Communications Board in the AVR and two remote input/output units

Design Function Identification:

The UFSAR describes the existence of two independent and redundant EDG trains, the EDG starting circuits and voltage and frequency control capability, the applicable design criteria and protective circuitry.

Screen Responses:

1. **Does the proposed activity involve a modification, addition to, or removal of a SSC such that the design function of the SSC, as described in the UFSAR, is adversely affected?**

   YES.

Combination of Components/Functions Assessment

The proposed activity does not involve the combination of components or functions, so there is *no adverse* impact on a design function due to combination-related issues.

Since identical software will be used in each digital AVR, there is an ***adverse*** impact on the independence of the EDGs described in the UFSAR.

Dependability Assessment

Since the digital AVR performs the exact same functions as the analog AVR, a direct correlation can be made by comparing the dependability of each device.

A commercial grade dedication (CGD) of the digital equipment was performed. The CGD demonstrated the digital equipment was equivalent to equipment developed under a 10 CFR 50, Appendix B QA program using a documented life-cycle process.

Based on the qualification activities and critical digital review documented in the CGD report, including software verification and validation, applicable operating history survey, the digital equipment is considered a highly reliable system on a level equal to, or exceeding, the analog equipment.

There is *no adverse* impact on a design function due to a reduction in the reliability of performing a design function.

2. Does the proposed activity involve a change to a procedure that adversely affects how UFSAR described SSC design functions are performed or controlled?

NO.

Physical Interface Assessment - Physical Interaction

No portion of the proposed activity involves how individuals interact with the new digital devices or the information presented by the new devices. Since no physical interface aspects are included in this change, *no adverse* impacts are possible.

Physical Interface Assessment - Number and/or Type of Parameters

The number and type of parameters described in the UFSAR for the analog control system will continue to be available with the digital control system. Therefore, *no adverse* impacts can be created due to the number and type of parameters associated with the digital control system.

Physical Interface Assessment - Information Presentation

The same information will be available with the new devices and the information will be used in the same manner.

Although the UFSAR describes the presence of an alarm in the control room, no design functions associated with the alarm (other than the obvious fact that the alarm provides information for the operator to perform certain actions) are specifically described regarding the use of an alarm versus any other type of instrumentation. Since no design functions are described, then *no adverse* impacts can be created.

The UFSAR describes the presence of instrumentation and annunciators provided to monitor EDG performance during normal and accident conditions. No design functions associated with the instrumentation and annunciators (other than the obvious fact that these devices provide information to the operator) are specifically described regarding the use of these devices versus any other type of device. Since no design functions are described, then *no adverse* impacts can be created.

EVALUATION

Criterion 2: **Does the proposed activity result in more than a minimal increase in the likelihood of occurrence of a malfunction of an SSC important to safety previously evaluated in the UFSAR?**

NO.

Level of Detail

The AVR is not explicitly described in the UFSAR, but is part of the EDG system. Therefore, the EDG system will be the appropriate level for which impacts on malfunction likelihood will be addressed.

The pertinent malfunctions previously evaluated in the UFSAR are detailed below:

(a) EDG System Electrical/Instrumentation Malfunctions Currently Described in the UFSAR

The UFSAR describes the malfunction of one EDG (to start when required).

(b) EDG System Malfunctions Currently Described in the UFSAR

The UFSAR states that no single failure can prevent EDGs from performing their safety function, including the ability to start when required and describes potential mechanical-related and electrical-related malfunctions.

Hazard Analysis

The FMEA of the new installation and concludes that this activity does not result in any new failure modes. The FMEA conservatively bounds the operating conditions of the EDGs during all modes of operation. A failure of one AVR does not affect the opposite AVR. Subsequent Factory Acceptance Testing in accordance with the Requirements Specification for Emergency Diesel Generator Excitation System confirmed that no additional digital-related failure modes are introduced by the software or hardware.

In the event of an AVR failure due to a design defect/latent error that is not identified by the rigorous V&V activities, automatic isolation of the AVR occurs and voltage control is transferred to the Magnetics voltage controller

before the EDG voltage exceeds Technical Specification limits. Devices used to isolate the AVR and allow only the Magnetics controller to control the EDG voltage are safety-related non-digital type relays with a fail-safe capacity to transfer to the Magnetics controller. A 3-second delay is provided to allow recovery from motor-start voltage transients for recovery of EDG voltage after a load step. Since the Magnetics alone will maintain the EDG output voltage within Technical Specification limits for the design basis LOOP event, there is no impact on the safety function of the EDG.

CCF Considerations - Hardware

The new AVR has been evaluated for CCF, with analysis that the likelihood of common cause failures from sources such as shared resources, environmental hazards, human error and other considerations for failure from a common source is unlikely. Each EDG is separated and isolated (physically and electrically) further reducing the susceptibility of a CCF due to environmental factors.

Based on this assessment, it can be reasonably concluded that a hardware-related CCF is *unlikely*.

CCF Considerations - Software

CGD of the software was performed to establish software quality and signify that the likelihood of a software defect is low. A critical digital review was performed, including an independent review of the software design and configuration process. The CGD process, which included the independent software review, demonstrated the software is equivalent to software developed under an Appendix B Quality Assurance Program. The device's application-specific configuration was performed using the site's Software Quality Assurance processes for safety-related digital devices.

Based on this assessment, it is concluded that a software-related CCF is *not unlikely*.

Justifications and Conclusions

The determination that a hardware-related CCF is *unlikely* is equivalent to a licensing condition of a malfunction that is NOT credible. Therefore, without a credible new malfunction initiator due to the hardware, there is not more than a minimal increase in the likelihood of a malfunction of an SSC important to safety previously evaluated in the UFSAR due to a hardware-related CCF.

The determination that a software-related CCF or a CCF resulting from a human error is *not unlikely* is equivalent to a licensing condition of credible and as likely to happen as those malfunctions described in the UFSAR. However, because the software was developed in accordance with a defined process, and complies with the applicable industry standards and regulatory guidance, the increase in the likelihood of a malfunction is not discernible (but is attributable to the proposed activity).

Since the increase in the likelihood of a malfunction is not discernible, there is not more than a minimal increase in the likelihood of a malfunction of an SSC important to safety previously evaluated in the UFSAR due to a software-related CCF.

Criterion 5: Does the proposed activity create a possibility for an accident of a different type than previously evaluated in the UFSAR?

NO.

The failure of the EDG is not an accident initiator, and as detailed above the possibility of failure of the AVR from a digital design defect or other failure, will not result in the loss of the EDG voltage control.

The determination that a hardware-related CCF is *unlikely* is equivalent to a licensing condition of an accident initiator that is NOT credible. Without a credible new accident initiator, a new accident cannot be created due to a hardware-related CCF. Therefore, if a new accident cannot be created, it is not possible to create an accident of a different type than previously evaluated in the USFAR due to a hardware-related CCF.

The determination that a software-related CCF is *not unlikely* is equivalent to a licensing condition of an accident initiator that IS credible. However, the EDG system is utilized in the mitigation of accidents and is not an initiator of any accident analyzed in the UFSAR. Furthermore, the proposed activity does not create a credible scenario in which the EDG system could become an accident initiator and voltage is maintained with the Technical Specifications limit consistent with the original design function. Therefore, without a credible scenario in which the new accident initiator would apply, it is not possible to create an accident of a different type than previously evaluated in the USFAR due to a software-related CCF.

Criterion 6: **Does the proposed activity create a possibility for a malfunction of an SSC important to safety with a different result than any previously evaluated in the UFSAR?**

NO.

Level of Detail

Same level as determined in the response to Criterion #2.

CCF Considerations - Hardware

Based on the assessment outlined in the response to Criterion #2, it was concluded that a hardware-related CCF was *unlikely*.

CCF Considerations - Software

Based on the assessment outlined in the response to Criterion #2, it was concluded that a software-related CCF was *not unlikely*.

Result

The UFSAR states "Each emergency generator...has the capacity, capability and reliability to provide on-site power for safe shutdown of the unit after loss of off-site power and meet the requirements of Regulatory Guide 1.9 and IEEE 387" and "...no single failure can prevent both emergency generator power systems from functioning. One emergency generator is adequate to supply power to all required emergency equipment."

Both of these UFSAR descriptions imply that only one of the two EDGs is needed. Therefore, the result is that one EDG will remain available.

Justifications and Conclusions

The determination that a hardware-related CCF is *unlikely* is equivalent to a licensing condition of a CCF malfunction that is NOT credible. Since a malfunction due to a hardware-related CCF is not credible, no results different from those previously evaluated in the UFSAR are possible.

The final AVR states that would occur from a software-related CCF due to a design defect in the operating system or in the application software are unknown. However, an analog relay mitigates the CCF by disconnecting the digital controller output from the exciter portion of the system when an upper

or lower voltage limit is exceeded. Upon disconnection, coarse voltage regulation remains available using components not involved with this proposed activity (instead of the fine voltage regulation that would be provided by the digital controller). The undervoltage and overvoltage setpoints of the analog relay provide assurance that the AVR digital controller will be disconnected before ESF bus voltage exceeds the Technical Specification limits required for powering ESF loads, and the coarse voltage regulation provided by the exciter portion of the system provides assurance that ESF bus voltage will remain within those limits. Since a software-related CCF of the AVR digital controllers will not cause the malfunction of an EDG (and the ESF loads served by the ESF busses, such that ESF equipment responses to transient and accident conditions assumed in the safety analysis will be unaffected), at least one EDG will remain available. With at least one EDG available, the result of a software-related CCF is the same as the result previously evaluated in the UFSAR.

Therefore, the replacement of the AVR analog controls with digital controls cannot create the possibility for a malfunction with a different result than that already considered in the UFSAR.

ALTERNATE Justifications and Conclusions for a Software-Related CCF

[*Author's Note: In this alternate response, which has been "fabricated" to cause an Evaluation conclusion that a License Amendment Request for the digital-related impacts IS required, the difference is the absence of the analog relay that mitigates the CCF. In this "fabricated" case, the response to this Criterion would be "YES."*]

The determination that a software-related CCF or a CCF resulting from a human error is *not unlikely* is equivalent to a licensing condition of a CCF malfunction that is as credible as those malfunctions described in the UFSAR.

The AVR states that would occur from a software-related CCF due to a design defect in the operating system or the application software are unknown. Given that the AVR states are unknown, the effect on EDG voltage regulation is also unknown. With an unknown effect on voltage regulation, the ability of the EDG to maintain voltage control within the Technical Specification limits required for powering ESF loads must be assumed to be exceeded (i.e., a new malfunction is created). This new malfunction causes both EDGs to be incapable of providing the electrical power required by multiple UFSAR descriptions.

Therefore, the replacement of the AVR analog controls with digital controls

creates the possibility for a malfunction with a different result than that already considered in the UFSAR, requiring submittal of a License Amendment Request.

5.7 EXAMPLE 6 - REPLACEMENT AND COMBINATION OF TWO CONTROL SYSTEMS

PURPOSE AND SUMMARY

The purpose of this example is to illustrate replacement of an analog control system with a digital control system for the non-safety-related feedwater control system, the replacement of an analog control system with a digital control system for the non-safety-related turbine control system, and the migration of these two previously independent control systems onto a Distributed Control System (DCS) platform (effectively combining these two previously separate control systems). Several HSI changes are involved in this activity.

As part of this activity, digital valve controllers will be installed on each feedwater control valve, creating the potential for a software common cause failure simultaneously affecting all valves, whereas the existing system design does not have this potential.

The Screen conclusion was *adverse* due to the digital-related impacts.

As part of this example, a portion of the response to Screen consideration #2 (procedures) will be modified to "fabricate" a Screen conclusion of adverse. This "fabricated" conclusion will be clearly indicated at the end of the response to Screen consideration #2 as "*ALTERNATE Justifications and Conclusions for Physical Interface Assessment - Physical Interaction.*" However, this "fabricated" adverse conclusion will not be addressed in the Evaluation.

In the Evaluation, hardware-related, network-related and human error-related CCF conclusions of *unlikely* and a software-related CCF conclusion of *not unlikely* were used from the technical support work. The Evaluation concluded that a License Amendment Request for the digital-related impacts was NOT required.

SCREEN

Title:

Replacement of Feedwater and Turbine Analog Control Systems with Digital Control Systems and Combination of Previously Separate Control Systems

Proposed Activity Description:

1. Feedwater Control System: There are two sets of feedwater regulating/bypass valves. Currently, each valve is controlled by a single analog controller. This activity replaces the single analog controller for each feedwater regulating and bypass valve with two (i.e., redundant) digital controllers. For each set of new digital controllers, one of the controllers will be "in service" while the other controller will be in "standby."

2. Turbine Control System: Replace the existing single analog controller that operates the four turbine throttle valve actuators with two (i.e., redundant) digital controllers. One of the new digital controllers will be "in service" while the other digital controller will be in "standby."

3. Distributed Control System: Connect the new feedwater and turbine digital controllers to the DCS network.

4. The operator interface for the feedwater and turbine control systems consist primarily of manual/auto (M/A) stations for manual control of each individual feedwater valve or the main turbine speed, as well as a manual turbine trip control. Aside from the plant computer, there is little information currently available to the operator with respect to these two systems. With the DCS, the M/A stations will be replaced with soft controls. The information available to the operator will increase tremendously – detailed graphics will be available for the feedwater and turbine control systems that currently do not exist. The new systems will be capable of providing alarming capabilities that did not exist with the current systems.

Design Function Identification:

Feedwater Control System:

The UFSAR indirectly identifies the feedwater control system as being independent from all other control systems and describes the operator interface as follows: "Sufficient instrumentation is provided to monitor and control automatically or manually the...Feedwater System under all operating conditions" and "...indicators are provided in the control room for the...feedwater control valve in each steam generator feedwater line."

Turbine Control System:

The UFSAR Section describes the design function of the turbine control system "to control the speed of the turbine when the generator is not synchronized with the system and to control the output of the unit when the generator is 'on line'," and indirectly identifies the turbine control system as being independent from all other control systems.

The UFSAR describes the operator interface as follows: The control panels for the DEH are located in the Control Room. The panels consist of electronic indicators, push button switches, signal lights to indicate the particular apparatus in control, and two reference displays to indicate the speed/MW reference and acceleration/MVAR values. Through keyboard push buttons, the operator can change the reference input to the electronic controller to vary the speed or load at different rates. Operator settings made at the panel are used by the electronic controller to position the steam valves by comparing the turbine speed or megawatt signals to the reference settings selected by the operator.

Screen Responses:

1. **Does the proposed activity involve a modification, addition to, or removal of a SSC such that the design function of the SSC, as described in the UFSAR, is adversely affected?**

   YES.

Combination of Components/Functions Assessment - Feedwater Control System

The proposed activity does not involve combination of components or functions, so there is *no adverse* impact on a design function due to combination-related issues.

Replacing each analog device with redundant digital devices *adversely* impacts the independence of the control systems described in the UFSAR because of the use of the same software in multiple feedwater control devices.

Combination of Components/Functions Assessment - Turbine Control System

None of the individual components are described in the UFSAR. Since none of the components are described in the UFSAR, then no design functions associated with those components can be described. Since no design functions are described, then *no adverse* impacts can be created.

Furthermore, there is *no adverse* impact on the overall design function described in the UFSAR (i.e., "... to control the speed of the turbine...") because no new malfunctions are created and no new accident initiators are created.

Combination of Components/Functions Assessment - DCS

Combining the previously independent feedwater control system and turbine control system *adversely* impacts the independence of the two control systems described in the UFSAR.

Dependability Assessment

Since the combined digital control system will perform the exact same functions as the separate analog control systems, a direct correlation can be made by comparing the dependability of each system.

The new digital control systems offer improvements in efficiency, reliability and availability compared to the legacy analog systems being replaced. The improvements are made possible (in part) by the use of redundant microprocessors, communication loops, power supplies, self-diagnostics, signal quality checking, automatic failover algorithms, and the elimination of several single points of vulnerability. Taken together, the proposed activity will yield a significant decrease in the frequency of failures leading to transients and moderate-frequency events previously analyzed in the UFSAR. This conclusion is supported by plant-specific reliability analyses that compare the legacy and upgraded control systems.

There is *no adverse* impact on a design function due to a reduction in the reliability of performing a design function.

2. Does the proposed activity involve a change to a procedure that adversely affects how UFSAR described SSC design functions are performed or controlled?

NO.

Physical Interface Assessment - Physical Interaction

Feedwater Control System: The physical interaction with the feedwater control system is not described in the UFSAR. Since no interactions are described in the UFSAR, then no design functions associated with those interactions can be described. Since no design functions are described, then *no adverse* impacts can be created.

Turbine Control System: Although the UFSAR describes several interactions with the turbine control system, no design functions are associated with the "push buttons" themselves (other than the obvious fact that the pushbuttons allow control). No design functions are specifically described regarding the interaction with a "pushbutton" versus any other type of interaction. Since control will still possible with the digital device, there is *no adverse* impact on the design function to provide a means of control.

Physical Interface Assessment - Number and/or Type of Parameters

Feedwater Control System: The number and type of parameters described in the UFSAR for the analog control system will continue to be available with the digital control systems. Therefore, *no adverse* impacts can be created due to the number and type of parameters associated with the digital control system.

Turbine Control System: The number and type of parameters described in the UFSAR for the analog control system will continue to be available with the digital control systems. Therefore, *no adverse* impacts can be created due to the number and type of parameters associated with the digital control system.

Physical Interface Assessment - Information Presentation

Feedwater Control System: Although the UFSAR describes the presence of "indicators," no design functions associated with the "indicator" (other than the obvious fact that the indicator provides information) are specifically described regarding the use of an "indicator" versus any other type of instrumentation. Since no design functions are described, then *no adverse* impacts can be created.

Turbine Control System: Although the UFSAR describes the presence of "indicators...signal lights...and...displays ," no design functions associated with these items (other than the obvious fact that the indicators provide information, the lights provide status and the displays provide information) are specifically described regarding the use of these items versus any other type of instrumentation, status indicators or display. Since no design functions are described, then *no adverse* impacts can be created.

ALTERNATE Justifications and Conclusions for Physical Interface Assessment - Physical Interaction

[*Author's Note: In this alternate response, which has been "fabricated" to cause an adverse impact for this Screen consideration, the difference is an*

operator interaction necessary to start a pump, resulting in a new failure mechanism. In this "fabricated" case, the response to this Screen consideration would be "YES."]

Existing Feedwater Pump Start Controls: To initiate a feedwater pump start using the existing analog control system, an operator depresses the associated feedwater pump start pushbutton on the main control board. Provided the system is correctly aligned (i.e., pump suction and discharge valves are open), the selected feedwater pump is started.

New Feedwater Pump Start Controls on the HSI: To initiate a feedwater pump start with the new digital control system, the operator must first "reset" the pump via the HMI. Selecting the wrong pump for reset would inadvertently reset the pump already in service, causing it to stop. This new manual control action, that can result in the unintended tripping of a running feedwater pump (i.e., a new failure), could not occur with the existing analog system. This new failure causes the *adverse* conclusion.

EVALUATION

Criterion 1: Does the proposed activity result in more than a minimal increase in the frequency of occurrence of an accident previously evaluated in the UFSAR?

NO.

[*Author's Note: In this example, all of the accidents are initiated by a malfunction of an SSC important to safety that has been previously evaluated in the UFSAR. Therefore, there is a direct relationship between the likelihood of occurrence of the malfunctions assessed in the response to Evaluation Criterion #2 and an increase in the frequency of the accidents in Evaluation Criterion #1.*]

The following UFSAR-described accidents are affected by the feedwater control system:

1. *Increase in Heat Removal by the Secondary System - Feedwater System Malfunction Causing an Increase in Feedwater Flow* (initiated by the full opening of one set of feedwater regulating/bypass valves)

2. *Decrease in Heat Removal by the Secondary System - Loss of Normal Feedwater* (initiated by the closure of all feedwater regulating valves)

The following UFSAR-described accidents are affected by the turbine control system:

1. *Increase in Heat Removal by the Secondary System - Excessive Increase in Secondary Steam Flow* (initiated by an unspecified malfunction of the turbine control system).

2. *Decrease in Heat Removal by the Secondary System - Turbine Trip* (initiated by the closure of all turbine control valves).

Since each accident is initiated by a "malfunction of an SSC important to safety previously evaluated in the UFSAR" and the conclusion in Criterion #2 was that the increase in the malfunction likelihood was "attributable, but not discernible," there is a corresponding "attributable, but not discernible" increase in the frequency of the affected accident (i.e., since the likelihood of the accident initiator does not increase, then the frequency of the accident does not increase either).

In the response to Criterion #5, the *Increase in Heat Removal by the Secondary System - Increase in Feedwater Flow* event [a frequency category II (Moderate Frequency) event] assuming the opening of both sets of feedwater regulating/bypass valves was determined to be bounded by the *Increase in Heat Removal by the Secondary System - Steam System Piping Failure* [a frequency category IV (Limiting Fault) event]. Even though a category II event was bounded by a category IV event, the frequency of the category II event is not affected. The frequency of the *Increase in Heat Removal by the Secondary System - Increase in Feedwater Flow* accident remains a frequency category II event because the increase in accident frequency was determined to be not more than minimal. Therefore, the accident frequency category for the *Increase in Heat Removal by the Secondary System - Increase in Feedwater Flow* event did not change from a less frequent accident category to a more frequent accident category.

Based on the assessments above, the proposed activity does not result in more than a minimal increase in the frequency of an accident previously evaluated in the UFSAR.

Criterion 2: **Does the proposed activity result in more than a minimal increase in the likelihood of occurrence of a malfunction of an SSC important to safety previously evaluated in the UFSAR?**

NO.

Level of Detail

The feedwater control system and the turbine control system are described in the UFSAR at ONLY the "system" level. Therefore, ONLY "system" level malfunctions will be considered in the development of the response.

Identification of Malfunctions

The following malfunctions (i.e., accident initiators) involving the feedwater control system have been previously evaluated:

1. In the UFSAR description of the *Increase in Heat Removal by the Secondary System - Feedwater System Malfunction Causing an Increase in Feedwater Flow* accident, excessive feedwater flow would result from the full opening of one set of feedwater regulating/bypass valves due to a feedwater control system malfunction.

2. In the UFSAR description of the *Decrease in Heat Removal by the Secondary System - Loss of Normal Feedwater* accident, the loss of all feedwater flow would result from the closing of all the feedwater regulating valves due to a feedwater control system malfunction.

The following malfunctions (i.e., accident initiators) involving the turbine control system have been previously evaluated:

1. In the UFSAR description of the *Increase in Heat Removal by the Secondary System - Excessive Increase in Secondary Steam Flow* accident, the increase in steam flow would result from the opening of the turbine control valves such that a 10 percent step load rated power increase occurs due to a turbine control system malfunction.

2. In the UFSAR description of the *Decrease in Heat Removal by the Secondary System - Turbine Trip* accident, the decrease in heat removal would result from the closing of all the turbine control valves due to a turbine control system malfunction.

Hazard Analysis

An FMEA and a Software Hazard Analysis (SHA) developed for the digital control systems revealed no single component or operating system failure that would detrimentally affect feedwater or turbine control system operation. Each control segment is provided with duplex controllers, one normally in-service and one on standby, a dedicated set of redundant I/O modules, redundant power supplies, a dedicated network, and dedicated

redundant I/O busses for communication between each controller and its associated I/O modules.

The feedwater control elements are further split into two separate segments, one per steam generator. As such, the result of a CCF due to a single controller failure or a single output module failure in a feedwater control segment remains bounded by the safety analysis (limited to spurious opening of the main and bypass valves on one steam generator).

The new digital control system offers redundancy and fault tolerance not obtainable with the existing analog system. Additionally, several single points of vulnerability found in the existing analog system have been eliminated.

CCF Considerations - Hardware

The new digital control system equipment installed by this activity has been analyzed to perform properly within the installed environment during normal operating conditions such that system performance will not be degraded compared to the control systems being replaced.

Digital systems are typically prone to failure modes caused by electromagnetic or radiofrequency interference (EMI/RFI). The new hardware has been hardened and tested to accepted industry standards for electromagnetic compatibility (EMC) in nuclear power plants. In addition, plant administrative procedures are in place to ensure that the control systems are not subjected to EMI/RFI beyond its capabilities. The major control functions performed by the systems are segregated onto different controller-pairs located in different cabinets, such that a failure induced by EMI/RFI will result in only one ANS Condition II plant transient. Therefore, the results of such malfunctions remain bounded by the results of the existing evaluations described in the UFSAR.

Based on this assessment, it can be concluded that a hardware-related CCF is *unlikely*.

CCF Considerations - Software

An NRC-endorsed industry standard provides an acceptable framework for planning and conducting a verification and validation program appropriately scaled to the software integrity level. The degree to which compliance with this industry standard has been achieved was evaluated to be appropriate considering the software integrity level in accordance with administrative procedures.

A quality assurance program (including use of industry-accepted software development process) is stipulated in the functional design specifications consistent with industry practice for non-safety instrumentation and control systems.

In the CCF Susceptibility Analysis, the likelihood of a software design defect simultaneously affecting two or more controllers is considered plausible (attributable); however, it is less likely than CCFs considered in the traditional safety analyses.

Based on this assessment, it is concluded that a software-related CCF is *not unlikely*.

CCF Considerations - Network Performance

Although the design provides a clock server on the Ethernet network for providing a date/time clock signal to each controller, the clock signal is not used in any control algorithms, ensuring the controllers will not be susceptible to erroneous conditions (caused by a clock failure) on the network interfaces. As such, a network clock error resulting in a CCF of the feedwater or turbine control valves is determined to be *unlikely*.

The DCS process network subnet switches and routers are configured for protection against data storms. Upon high port utilization, the affected switch/router will throttle the amount of data passed through the port ultimately preventing the data storm from propagating through the network to other controllers. Factory and site acceptance testing using an externally generated data storm confirmed that the network switches/routers, as configured, prevent the data storm from propagating through the network to other controllers. Therefore, a data storm resulting in a CCF of the feedwater or turbine control valves is determined to be *unlikely*.

CCF Considerations - Human Performance

The proposed activity requires reevaluation of the control room HSI for adequacy using industry accepted human factors engineering (HFE) standards. The methodology used to perform the original control room design review followed current NRC guidance at that time. The methodology used to evaluate the modified control room HSI follows current NRC guidance.

Based on this assessment, the likelihood of a CCF due to human error is determined to be *unlikely*.

Justifications and Conclusions

The determination that a hardware-related CCF or a CCF resulting from a network or human error is *unlikely* is equivalent to a licensing condition of a malfunction that is NOT credible. Therefore, without a credible new malfunction initiator due to the hardware, human error or a network error, there is not more than a minimal increase in the likelihood of a malfunction of an SSC important to safety previously evaluated in the UFSAR due to a hardware-related CCF.

The determination that a software-related CCF is *not unlikely* is equivalent to a licensing condition of a malfunction that IS credible. However, because the software was developed in accordance with a defined process, an increase in the likelihood of a malfunction previously evaluated in the UFSAR is not discernible (but is attributable to the proposed activity). Therefore, since an increase in the likelihood of a malfunction is not discernible, there is not more than a minimal increase in the likelihood of a malfunction of an SSC important to safety previously evaluated in the UFSAR due to a software-related CCF.

Criterion 5: Does the proposed activity create a possibility for an accident of a different type than previously evaluated in the UFSAR?

NO.

CCF Considerations - Hardware

Based on the assessment outlined in the response to Criterion #2, it was concluded that a hardware-related CCF was *unlikely*.

CCF Considerations - Software

Based on the assessment outlined in the response to Criterion #2, it was concluded that a software-related CCF was *not unlikely*.

CCF Considerations - Network Performance

Based on the assessment outlined in the response to Criterion #2, it was concluded that a data communication design defect CCF was *unlikely*.

CCF Considerations - Human Performance

Based on the assessment outlined in the response to Criterion #2, it was

concluded that the likelihood of a CCF due to human error was *unlikely*.

Accident Identification

A review of the UFSAR identified the following pertinent accidents that have been previously evaluated:

1. *Increase in Heat Removal by the Secondary System - Feedwater System Malfunction Causing an Increase in Feedwater Flow* (initiated by the full opening of one set of feedwater regulating/bypass valves).

2. *Increase in Heat Removal by the Secondary System - Excessive Increase in Secondary Steam Flow* (initiated by an unspecified malfunction of the turbine control system).

3. *Decrease in Heat Removal by the Secondary System - Turbine Trip* (initiated by the closure of all turbine control valves)

4. *Decrease in Heat Removal by the Secondary System - Loss of Normal Feedwater* (initiated by the closure of all feedwater regulating valves)

Multiple Accident Assessment

Due to segmentation of the controllers, use of different application code software in the feedwater and turbine control systems and different inputs into the feedwater and turbine control systems, there are no possible CCFs that can cause multiple accidents to occur (e.g., *Loss of Normal Feedwater* AND *Excessive Increase in Secondary Steam Flow*).

Bounding Assessment

Given that the only outcomes from a software-related CCF are accident initiators that can cause an increase or decrease in heat removal by the secondary system, no new accidents are created.

Justifications and Conclusions

The determination that a hardware-related CCF or a CCF resulting from a network or human error is *unlikely* is equivalent to a licensing condition of an accident initiator that is NOT credible. Without a credible new accident initiator, a new accident cannot be created due to a hardware-related CCF or a CCF resulting from a network or human error. Therefore, since a new accident cannot be created, it is not possible to create an accident of a different type than previously evaluated in the USFAR due to a hardware-

related CCF or a CCF resulting from a network or human error.

The determination that a software-related CCF is *not unlikely* is equivalent to a licensing condition of an accident initiator that IS credible. However, the accident initiators cause accidents previously considered in the UFSAR. Therefore, this activity will not create the possibility for an accident of a different type than previously evaluated in the UFSAR.

Criterion 6: **Does the proposed activity create a possibility for a malfunction of an SSC important to safety with a different result than any previously evaluated in the UFSAR?**

NO.

Level of Detail

Same level as determined in the response to Criterion #2.

[*Author's Note: The malfunction "results" have been indicated using double underline for emphasis.*]

The feedwater control system malfunctions and results previously evaluated in the UFSAR are identified below:

1. Feedwater control system malfunction that opens a feedwater bypass valve, diverting flow around a portion of the feedwater heaters, and causing a reduction in feedwater temperature.

2. Feedwater control system malfunction that opens a feedwater regulating valve, creating (a) a greater load demand on the RCS (at power) due to increased subcooling in the steam generator, or (b) decreases RCS temperature and a positive reactivity insertion due to the effects of the negative moderator coefficient of reactivity (at no-load conditions).

3. Feedwater control system malfunctions that closes all feedwater regulating valves, causing a reduction in the capability of the secondary system to remove the heat generated in the reactor core.

In addition to the previously evaluated feedwater control system malfunctions identified above, a new postulated malfunction (CCF) in the digital feedwater control system could occur.

The turbine control system malfunction and results previously evaluated in the UFSAR are identified are described in the UFSAR as follows: a turbine control system malfunction that opens all turbine control valves, causing an excessive increase in secondary steam flow, leading to a mismatch between the reactor core power and the steam generator load demand.

CCF Considerations - Hardware

Based on the assessment outlined in the response to Criterion #2, it was concluded that a hardware-related CCF was *unlikely*.

CCF Considerations - Software

Based on the assessment outlined in the response to Criterion #2, it was concluded that a software-related CCF was *not unlikely*.

CCF Considerations - Network Performance

Based on the assessment outlined in the response to Criterion #2, it was concluded that a data communication design defect CCF was *unlikely*.

CCF Considerations - Human Performance

Based on the assessment outlined in the response to Criterion #2, it was concluded that the likelihood of a CCF due to human error was *unlikely*.

Results Assessment

Previously Evaluated Results:

Most of the results described above are "intermediate" results and will not be addressed in this response.

However, the "end" result in each case is the amount of heat removed by the secondary system. Namely, either an increase or decrease in heat removal occurs.

New Results:

Decrease in Heat Removal New Result:

Since the loss of all feedwater and the "end" result of such a malfunction on the decrease in heat removal has been previously considered in the licensing basis, there cannot be a different result for the "decrease" event.

Increase in Heat Removal New Result #1:

As described in the UFSAR, the *Increase in Heat Removal by the Secondary System - Steam System Piping Failure* event is the most limiting cooldown transient.

A re-analysis of the *Increase in Heat Removal by the Secondary System - Increase in Feedwater Flow* event was performed assuming the opening of both sets of feedwater regulating/bypass valves.

The applicable analytical result from the *Increase in Feedwater Flow* event re-analysis is the minimum value of DNBR. The minimum DNBR value from the re-analysis was demonstrated to be greater than the minimum DNBR value from the *Steam System Piping Failure* event (i.e., was bounded).

Increase in Heat Removal New Result #2:

As described in the UFSAR, the *Increase in Heat Removal by the Secondary System - Excessive Increase in Secondary Steam Flow*, an excessive increase in secondary system steam flow is defined as a rapid increase in steam flow that causes a power mismatch between the reactor core power and the steam generator load demand. The Reactor Control System is designed to accommodate a 10 percent step load increase or a 5 percent per minute ramp load increase in the range of 15 to 100 percent of full power. UFSAR Section 15.1.3.2 states that the analysis will "demonstrate the plant behavior following a 10 percent step load increase from rated load." Therefore, although the actual number of turbine control valves malfunctioning is not considered in the analysis, if a malfunction that causes the opening of all the turbine control valves does not cause more than a "10 percent step load increase," then the new accident would be bounded by the accident previously evaluated in the UFSAR.

A re-analysis of the *Increase in Heat Removal by the Secondary System - Excessive Increase in Secondary Steam Flow* event, assuming the opening of all turbine control valves, was performed.

The outcome from the re-analysis indicated that a step load increase of 9.65 percent, satisfying the 10 percent step load assumption.

Comparison of Results:

All of the new end results are bounded by the results previously evaluated in the UFSAR.

Justifications and Conclusions

The determination that a hardware-related CCF or a CCF resulting from a network or human error is *unlikely* is equivalent to a licensing condition of a CCF malfunction that is NOT credible. Since a malfunction due to a hardware-related CCF or a CCF resulting from a network or human error is not credible, no results different from those previously evaluated in the UFSAR are possible.

The determination that a software-related CCF is *not unlikely* is equivalent to a licensing condition of a CCF malfunction that is as credible as those malfunctions described in the UFSAR. The feedwater and turbine control system malfunction results at the plant level are bounded by the malfunction results previously evaluated in the UFSAR at the plant level.

Thus, this activity will not create the possibility for a malfunction of either the feedwater or turbine control systems with a different result than any previously evaluated in the UFSAR.

5.8 EXAMPLE 7 - COMBINATION OF COMPONENTS AND FUNCTIONS

PURPOSE AND SUMMARY

This example illustrates a digital modification that combines components and functions. No new digital hardware is being added and no HSI modifications are involved.

The Screen conclusion was *adverse* due to the creation of a new malfunction from the combination of components and functions.

In the Evaluation, the creation of a new malfunction caused a discernible increase in the likelihood of a malfunction previously evaluated in the UFSAR and created the possibility for a malfunction of an SSC important to safety with a different result than any previously evaluated in the UFSAR. The Evaluation concluded that a License Amendment Request (LAR) is required.

SCREEN

Title:

Replacement of Feedwater Control Valve and Feedwater Bypass Valve Mechanical Limit Switches with Digital Valve Controller Data

Proposed Activity Description:

1. Combination of Components and Functions

   Background:

   Digital valve positioners on each main feedwater control and bypass valve provide valve position feedback to the digital feedwater control system for steam generator level control. In addition, each feedwater control valve and each feedwater bypass valve has two sets of mechanical limit switches. One set of limit switches is used to provide valve position information to the plant computer and the main control board indications. The other set of limit switches is used to provide valve position input to the Anticipated Transient Without Scram (ATWS) Mitigation System and Actuation Circuitry (AMSAC).

Modification:

For each valve, remove both sets of mechanical limit switches and utilize digital output modules from the digital feedwater control system to provide feedwater valve position information to the plant computer, the main control board indication and to the AMSAC.

[*Author's Note: To illustrate how an activity other than that directly related to the harware, software or HSI aspects can accompany a digital modification, the activity identified in #2 below is part of the overall modification. However, this activity is not unique to "digital" since this type of activity could have been implemented with a non-digital modification. This portion of the proposed activity will not be addressed in this example, which focuses only on the strictly digital aspects of the modification. In an actual Screen, this portion of the proposed actvity would need to be addressed.*]

2. Fundamental Change to How a Function is Performed

   The modification also entails a fundamental change to how the valve position determination function is performed – from physical proximity (i.e., physical interaction of the valve position contact arm with the limit switch) to digital calculation (using valve position data provided by the digital feedwater control system).

Design Function Identification:

Anticipated Transient Without Scram (ATWS) Mitigation System and Actuation Circuitry (AMSAC):

Position of the main feedwater control valves, feedwater control valve bypass valves and main feedwater isolation valves is monitored by limit switches on the valves. These switches are set to enable the AMSAC circuitry when a control valve in a main feedwater flow path is less than 25% open (i.e., the lower limit switch has been actuated), with the associated control valve bypass valve less than 100% open (i.e., the upper limit switch is NOT actuated).

Minimum AMSAC flow requirements can be maintained with the control valve closed and the control valve bypass valve fully open. The control valve indication is interlocked with the bypass valve indication such that both the control valve and the bypass valve must be closed to the stated setpoints to indicate a blocked flow path.

Screen Responses:

1. **Does the proposed activity involve a modification, addition to, or removal of a SSC such that the design function of the SSC, as described in the UFSAR, is adversely affected?**

   YES.

Combination of Components/Functions Assessment

Currently, the digital feedwater control system and the valve mechanical limit switches are physically separate components. A malfunction (due to any cause) in one component (e.g., the digital control system) cannot impact the performance of the other component (e.g., the mechanical limit switch). With the proposed design, a malfunction of the digital device (due to any cause) can now also impact the valve position information. If the valve position information can be affected, the AMSAC system could be actuated when it should not have been actuated or, the AMSAC system could fail to be actuated when it should have been actuated. Neither of these postulated ASMAC responses was previously possible.

Removing the limit switches and migrating the function of the limit switches to the digital control system *adversely* impacts the independence of the limit switches described in the UFSAR because the potential for new malfunctions that did not previously exist has been created.

2. **Does the proposed activity involve a change to a procedure that adversely affects how UFSAR described SSC design functions are performed or controlled?**

   NO.

No portion of the proposed activity involves how individuals interact with the new digital devices or the information presented by the new devices. The same information will be available with the new devices and the information will be used in the same manner. Since no HSI aspects are included in this change, *no adverse* impacts are possible.

EVALUATION

Criterion 2: **Does the proposed activity result in more than a minimal increase in the likelihood of occurrence of a malfunction of an SSC important to safety previously evaluated in the UFSAR?**

YES.

Level of Detail

The mechanical limit switches and the AMSAC system are described in the UFSAR. Therefore, both of these "levels" will be considered in the development of the response.

Identification of Malfunctions

No direct malfunctions of either the limit switches or the AMSAC system are described in the UFSAR.

However, an indirect description involving the limit switches is described, as follows: "Position of the main feedwater control valves, feedwater control valve bypass valves and main feedwater isolation valves is monitored by limit switches on the valves. These switches are set to enable the AMSAC circuitry when a control valve in a main feedwater flow path is less than 25% open (i.e., the lower limit switch has been actuated), with the associated control valve bypass valve less than 100% open (i.e., the upper limit switch is NOT actuated). Therefore, the control valve indication is interlocked with the bypass valve indication such that both the control valve and the bypass valve must be closed to the stated setpoints to indicate a blocked flow path. If 3 out of 4 flow paths are blocked, the AMSAC circuitry will actuate."

In this description, since signals from only "3 out of 4" limit switches are necessary for the AMSAC circuitry to actuate, the malfunction of the "fourth" limit switch is accommodated.

CCF Considerations - Hardware

No new hardware is installed as part of the proposed activity. Therefore, consideration of a hardware-related CCF is not necessary.

CCF Considerations - Software

In accordance with Example 6 in Section 4.3.2 of the main body of NEI 96-07, the creation of a new malfunction (i.e., a software-related CCF affecting the valve position information used in the actuation of the AMSAC system) due to the reduction in equipment independence causes a discernible increase in the likelihood of a malfunction.

Justifications and Conclusions

As stated above, no new hardware is installed as part of the proposed activity. Therefore, consideration of a hardware-related CCF is not necessary. Without a credible new malfunction initiator due to the hardware, there is not more than a minimal increase in the likelihood of a malfunction of an SSC important to safety previously evaluated in the UFSAR due to a hardware-related CCF.

In accordance with Example 6 in Section 4.3.2 of the main body of NEI 96-07, the creation of a new malfunction due to a reduction in equipment independence causes a discernible increase in the likelihood of a malfunction. Since an increase in the likelihood of a malfunction is discernible, there is more than a minimal increase in the likelihood of a malfunction of an SSC important to safety previously evaluated in the UFSAR due to a software-related CCF, requiring submittal of a License Amendment Request.

Criterion 5: Does the proposed activity create a possibility for an accident of a different type than previously evaluated in the UFSAR?

NO.

No new hardware is installed as part of the proposed activity. Therefore, consideration of a hardware-related CCF is not necessary. Without a credible new accident initiator, a new accident cannot be created due to a hardware-related CCF. Therefore, since a new accident cannot be created, it is not possible to create an accident of a different type than previously evaluated in the USFAR due to a hardware-related CCF.

Should a software-related CCF occur that causes AMSAC to actuate when it should not have, a turbine trip will be initiated. However, the Loss of Load event (initiated from a turbine trip) is an accident that has been previously evaluated in the UFSAR. Therefore, it is not possible to create an accident of a different type than previously evaluated in the USFAR due to a software-related CCF.

Criterion 6: **Does the proposed activity create a possibility for a malfunction of an SSC important to safety with a different result than any previously evaluated in the UFSAR?**

YES.

Level of Detail

Same level as determined in the response to Criterion #2.

[*Author's Note: The malfunction "results" have been indicated using double underline for emphasis.*]

The following malfunction and results previously evaluated in the UFSAR are identified below:

Following the failure of the Reactor Protection System (RPS) to trip the reactor (i.e., malfunction of the RPS; namely, an ATWS), a series of generic studies on limiting ATWS events for Westinghouse plants showed that acceptable plant response would result provided that the turbine trips and auxiliary feedwater flow is initiated in a timely manner.

In addition to the previously evaluated RPS malfunction identified above, a new postulated malfunction (i.e., a software CCF) in the digital feedwater control system could occur, causing the AMSAC system to be actuated when it should not have been actuated or the AMSAC system to not actuate when it should have been actuated.

Results Assessment

Previously Evaluated Result:

The previously evaluated result is acceptable plant response.

New Results:

The new results are unacceptable plant response. For the case in which the AMSAC system was actuated when it should not have been, tripping the turbine and initiating auxiliary feedwater flow when neither action was necessary creates an unacceptable plant response. For the case in which the AMSAC system was not actuated when it should have been, the ATWS condition is not recognized and the required actions of tripping the turbine

and initiating auxiliary feedwater flow are not performed, each of which is described in the UFSAR.

Comparison of Results:

The new results are NOT bounded by the results previously evaluated in the UFSAR.

Justifications and Conclusions

No new hardware is installed as part of the proposed activity. Therefore, consideration of a hardware-related CCF is not necessary. Without a credible malfunction initiator due to the hardware, no results different from those previously evaluated in the UFSAR are possible.

The determination that a software-related CCF is *not unlikely* is equivalent to a licensing condition of a CCF malfunction that is as credible as those malfunctions described in the UFSAR. However, the digital feedwater control system malfunction results are NOT bounded by the malfunction results previously evaluated in the UFSAR.

Thus, this activity creates the possibility for a malfunction of the feedwater control systems with a different result than any previously evaluated in the UFSAR, requiring submittal of a License Amendment Request.