NEI PROPOSED REVISIONS
(Document Date: December 20, 2016)

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.

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

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 or controlled. The mere fact that a digital processor "calculates" a numerical value or "generates" a control signal using software is not fundamentally different from a numerical value or a control signal using analog components if the digital device (hardware and software) cannot produce erroneous numerical values or control signals due to failures any different from those produced by the analog devices. Similarly, the mere fact that a touchscreen may be used in place of hard controls (i.e., pushbuttons, knobs, switches, etc.) to operate or control plant equipment is not fundamentally different from the hard controls if the digital device (hardware and software) cannot produce erroneous operations or controls due to failures any different from those produced by the analog devices.

Examples are provided to illustrate the guidance provided in this document. Unless stated otherwise, a given example only addresses the aspect or topic within the

section/sub-section in which it is included, sometimes at the deliberate exclusion of other aspects or topics that, if considered, could potentially change the Screen conclusion

Commented [D1]: Addresses NRC item 10

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., flow measurement) 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 analog control systems, one for each MFWP, that are both physically and functionally the same. 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*. Each of these activities involves a fundamental change since each creates the potential for new malfunctions that were not previously considered.

Commented [D2]: Addresses NRC item 7

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.

NEI PROPOSED REVISIONS
(Document Date: December 20, 2016)

3.2 PROCESS

Generally, a digital modification consists of three general areas of activities: (1) software-related, (2) hardware-related and (3) Human-System Interface-related. The software and hardware portions will be assessed within the "facility" Screen consideration and the Human-System Interface portion will be assessed within the "procedures" Screen consideration.

Commented [D3]: Addresses NRC item 9

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.

Although a "graded approach" to addressing software in a 50.59 review is not directly possible (e.g., unique criteria cannot be developed for safety-related SSCs vs. non-safety-related SSCs; as exists for some technical considerations), the SSCs and functions to which 50.59 applies can be used as a process for eliminating SSCs and non-design functions from consideration in a 50.59 review.

From NEI 96-07, Section 3.3., the following two excerpts are repeated due to their significance in identifying a "graded approach."

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

and

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

In each of these excerpts, the general 50.59 guidance makes it clear that a form of "graded approach" exists and as based on the SSCs and the specific type of functions (i.e., "design functions," not ALL functions) that are considered to be within the scope of a 50.59 review. For digital modifications, the 50.59 practitioner would greatly benefit from a complete and thorough understanding of the SSC(s) and types of function(s) involved with a digital modification and, particularly, those involved with the introduction of software.

This understanding could help in eliminating the application of 50.59 when 50.59 does not apply.

Commented [D4]: Addresses NRC item 2

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

(a) SSC Characteristics

(b) Combination of Components/Functions

(c) Dependability

3.2.1.2 SSC Characteristics

During the original licensing process, the characteristics of SSCs in the facility may have been a consideration. ~~In general, different SSCs may be equivalent, similar or identical to one another physically or functionally.~~

Commented [D5]: NEI-initiated to complete removal of previously proposed language

The UFSAR may explicitly or implicitly describe the characteristics of SSCs through diversity, separation, independence and/or redundancy discussions. With digital modifications, the new equipment has the potential to impact the diversity, separation, independence and/or redundancy of the SSCs described in the UFSAR.

To assist in determining the impact of a digital modification on the diversity, separation, independence and/or redundancy of the affected components, identify the characteristics of SSCs described in the UFSAR. Compare the proposed characteristics of SSCs with the existing characteristics of SSCs. The impact of any differences in the characteristics of SSCs on diversity, separation, independence and/or redundancy is then determined.

For redundant SSCs that must satisfy single failure criteria requirements, the following guidance applies:

1. The use of the same software in two or more redundant SSCs is ADVERSE because the independence of the SSCs has been reduced.

2. The use of different software in two or more redundant SSCs is NOT ADVERSE because the independence of the SSCs has been maintained.

~~3. The use of exactly the same or different hardware in two or more redundant SSCs is subject to the same licensing considerations as described in the UFSAR as those for non-digital SSCs and a conclusion of ADVERSE or NOT ADVERSE is determined in the same manner as for non-digital proposed activities.~~

Commented [D6]: NEI-initiated to remove guidance not unique to digital

Example 3-3 illustrates the application of the *SSC characteristics* aspect.

Example 3-3. NO ADVERSE IMPACT on a UFSAR-Described Design Function

related to SSC Characteristics

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

The licensee proposes to replace the two analog control systems with two digital control systems. The hardware platform for each digital control system is from the same supplier and the software in each digital control system is exactly the same.

The pertinent UFSAR descriptions are as follows:

(1) Two analog control systems are described.

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

(3) The described MFWP control system malfunctions include (a) failures causing the loss of all feedwater to the steam generators and (b) failures causing an increase in main feedwater flow to the maximum output from both MFWPs.

The use of the same hardware platforms and same software in both control systems is NOT ADVERSE for the following reasons:

(1) The concept of redundancy to address single failure considerations does not apply. There are no UFSAR descriptions related to the ability of one MFWP and its analog control system to provide a redundant source of main feedwater flow in the event of the loss of the other MFWP/control system. Therefore, the MFWPs and control systems are not required to satisfy single failure criteria. The two analog control systems existed for operational convenience only, not to satisfy any General Design Criteria requirements.

Commented [D7]: NEI-initiated to improve clarity

(2) There is no impact on diversity since none originally existed or was described in the UFSAR.

(3) There is no impact on the separation of the control systems described in the UFSAR since each of the analog control systems will be replaced with its own digital control system.

(4) Although both of the new digital control systems contains the exact same software (which is subject to a software CCF), no new types of malfunctions are introduced since the loss of both MFWPs and failures causing an increase in main feedwater flow to the maximum output from both MFWPs are already considered in the licensing basis.

NOTE: If the UFSAR described the loss of only ONE MFWP, the proposed activity would be ADVERSE because a new type of malfunction would be introduced due to a possible software CCF that could disable BOTH MFWPs. Similarly, if the UFSAR described the consideration of the maximum output from only ONE MFWP, the

proposed activity would be ADVERSE because a new type of malfunction would be introduced due to a possible software CCF that could cause BOTH MFWPs to reach their maximum output.

Commented [D8]: Addresses NRC item 7

~~***Example 3-4. Replacing SSC Types with an ADVERSE IMPACT on a UFSAR-Described Design Function***~~

~~Using the same basic information from Example 3-3, this example illustrates how variations in the licensing basis as described in the UFSAR would result in ADVERSE conclusions.~~

~~Alternate Licensing Basis #1: If the UFSAR described the loss of only ONE MFWP, the proposed activity would be ADVERSE because a new type of malfunction would be introduced due to a possible software CCF that could disable BOTH MFWPs.~~

~~Alternate Licensing Basis #2: If the UFSAR described the consideration of the maximum output from only ONE MFWP, the proposed activity would be ADVERSE because a new type of malfunction would be introduced due to a possible software CCF that could cause BOTH MFWPs to reach their maximum output.~~

Commented [D9]: NEI-initiated to include this information in Example 3-3

3.2.1.3 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 considered in the process of identifying possible malfunctions or accident initiators that could exist.

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

The combination of previously separate components and/or functions, in and of itself, does not make the Screen conclusion adverse. Only if combining the previously separate components and/or functions causes a reduction in the SSC's ability or capability of performing a design function (e.g., by the creation of a new malfunction or the creation of a new accident initiator) is the combination aspect of the digital modification adverse.

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

Examples 3-4 through 3-7 illustrate the application of the *combination of components/functions* aspect.

Example 3-4. Combining Components and Functions with NO ADVERSE IMPACT on a UFSAR-Described Design Function

A licensee has two non-safety-related main feedwater pumps (MFWPs). There are two analog control systems (one per MFWP) that are physically and functionally the same. System drawings (incorporated by reference into the UFSAR) show that each analog control system has many subcomponents performing dedicated functions.

The licensee proposes to replace all of the analog subcomponents with a single digital device that consolidates all of the components, sub-components and the functions associated with each component and sub-component. Each analog control system will be replaced with a separate digital control system. The hardware platform for each digital control system is from the same supplier and the software in each digital control system is exactly the same. ~~There are no interactions between the two new digital control systems or any other plant component(s) that did not previously exist.~~

Commented [D10]: NEI-initiated as not being related to the aspect being illustrated

The pertinent UFSAR descriptions are as follows:

(1) Two analog feedwater control systems are described, but none of the individual components or subcomponents are described. The feedwater control system contains a design function "to provide adequate cooling water to the steam generators during normal operation."

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

(3) The described MFWP control system malfunctions include (a) failures causing the loss of <u>all</u> feedwater to the steam generators and (b) failures causing an increase in main feedwater flow to the maximum output from both MFWPs.Since only the control system is described in the UFSAR, it is the only SSC to be examined for the identification of design functions. [NOTE: The purpose of the system "*to provide adequate cooling water to the steam generators during normal operation*" 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 the following 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 subcomponent, 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)~~ No new malfunctions are created. The only malfunctions of interest are related to the common cause failure of both control systems, which can result in either the loss of all feedwater flow or the allowance of maximum feedwater flow, both of which have been previously considered in the licensing basis. Since no new malfunctions are created, the ability to perform the design function "to provide adequate cooling water to the steam generators during normal operation" is maintained.

Commented [D11]: NEI-initiated to focus on the aspect being illustrated

Example 3-5. Combining Components and Functions with NO ADVERSE IMPACT on a UFSAR-Described Design Function

Using the same initial facility configuration, proposed activity and UFSAR descriptions from Example 3-4, this example illustrates how a variation in the proposed activity would be addressed.

Commented [D12]: Addresses NRC item 7

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 due to consideration of the combination aspect 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 been previously considered in the licensing basis). Since no new malfunctions are created, the ~~reliability~~ability of the design function "to provide adequate cooling water to the steam generators during normal operation" is maintained.

Commented [D13]: NEI-initiated to add clarity

Commented [D14]: Addresses NRC item 5

Example 3-6. Combining Components and Functions with an ADVERSE IMPACT on a UFSAR-Described Design Function

Using the same initial facility configuration and proposed activity from Example 3-4, this example illustrates how a variation in the licensing basis as described in the UFSAR impacts the Screen conclusion, causing an adverse impact.

Licensing Basis as Described in the UFSAR: 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.

Commented [D15]: Addresses NRC item 7

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 3-5 was proposed (i.e., the 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~~ ability of the design function "to provide adequate cooling water to the steam generators during normal operation."

Commented [D16]: Addresses NRC item 5

Example 3-7. Combining Components and Functions with an ADVERSE IMPACT on a UFSAR-Described Design Function

~~Using the same initial facility configuration from Example 3-4, 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.~~

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

Commented [D17]: Addresses NRC item 7

The licensee proposes to combine the two feedwater control systems and the main turbine steam-inlet valves control system into a single digital device.

~~The design function for the feedwater control system from Example 3-5 remains pertinent. Since only the turbine steam-inlet control valve control system is described in the UFSAR, it is the only other 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. However, 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.~~

The pertinent UFSAR descriptions are as follows:

(1) Two analog feedwater control systems are identified. The feedwater control system contains a design function "to provide adequate cooling water to the steam generators during normal operation." [NOTE: The purpose of the system "*to provide adequate cooling water to the steam generators during normal operation*" 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 or Excess Feedwater).]

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

(3) The described feedwater control system malfunctions include (a) failures causing the loss of all feedwater to the steam generators and (b) failures causing an increase in main feedwater flow to the maximum output from both MFWPs.

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

(5) Note that the licensing basis does not consider a simultaneous Loss of Feedwater accident or Excess Feedwater accident with either the Excess Steam Demand accident or the Loss of Load accident.

Commented [D18]: Addresses NRC item 7

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 separation described in the UFSAR.~~

Commented [D19]: NEI-initiated to focus on the aspect being illustrated

This impact has an adverse impact on ~~reliability~~ the ability of the feedwater control system design function "to provide adequate cooling water to the steam generators

Commented [D20]: Addresses NRC item 5

during normal operation" and the ~~reliability~~ ability of the turbine control system design function "to control the amount of steam entering the main turbine during normal operation."

Commented [D21]: Addresses NRC item 5

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..."

Note that as used in this context, "reliability" refers to the ability or capability of a design function being performed as described, NOT the technical reliability of the SSC itself being able to operate. Namely, an SSC could fail 100% of the time, but if it's design function was to "not respond" then it would continue to perform its design function regardless of its operational state.

~~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.~~

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

Commented [D22]: Addresses NRC items 1 and 4

Example 3-8. Digital Modification that Satisfies Dependability, causing NO ADVERSE IMPACT on a UFSAR-described Design Function

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

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

The licensee concludes that the change will not adversely affect any design function and screens out the change.

Commented [D23]: Addresses NRC item 6

3.2.2 SCREENING OF CHANGES TO PROCEDURES AS DESCRIBED IN THE UFSAR

In the main body of NEI 96-07, Section 3.9 defines *procedures* as follows:

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

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

If the digital modification does not involve or include a Human-System Interface (e.g., the replacement of an analog relay with a digital relay that has no features involving personnel interaction), then this section does not apply and may be excluded from the Screen assessment.

Commented [D24]: Addresses NRC items 8 and 9

3.2.2.1 SCOPE

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

The focus of the Screen assessment is on potential adverse effects due to modifications of the *interface* between the human user and the technical device [e.g., equipment manipulations, actions taken, options available, manipulation sequences or operator response times (including the impact of errors of a cognitive nature in which the information being provided is unclear or incorrect)], not the written procedure modifications that may accompany a physical design modification (which are addressed in the guidance provided in the main body of NEI 96-07, Revision 1, section 4.2.1.2).

Commented [D25]: NEI-initiated to provide clarification

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

(a) Physical Interaction

(b) Number/Type of Parameters

(c) Information Presentation

(d) Operator Response Time

Commented [D26]: NEI-initiated for completeness

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

- Changes to parameters monitored, decisions made, and actions taken in the control of plant equipment and systems during transients.
- Changes that could affect the overall response time of the human/machine system (e.g., changes that increase operator burden).
- Changes from manual to automatic initiation (or vice versa) of functions.
- Fundamental changes in data presentation (such as replacing an edgewise analog meter with a numeric display or a multipurpose CRT where access to the data requires operator interactions to display), or

- Changes that create new potential failure modes in the interaction of operators with the system (e.g., new interrelationships or interdependencies of operator actions and plant response or new ways the operator assimilates plant status information).

If the HSI changes do not exhibit these characteristics, then it may be reasonable to conclude that the "method of performing or controlling" the design function is not adversely affected.

Commented [D27]: Addresses NRC item 11

3.2.2.2 PHYSICAL INTERFACE

Physical Interaction

Consideration of a digital modification's impact on the 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").

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 the use of a touch screen in place of push-buttons, switches or knobs.

Examples 3-9 through 3-11 illustrate the application of the *physical interaction* aspect.

Example 3-9. Physical Interaction with NO ADVERSE IMPACT on a UFSAR-Described Design Function

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

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

Examining only the physical interaction 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 3-10. Physical Interaction with an ADVERSE IMPACT on a UFSAR-Described Design Function

Using the same proposed activity described in Example 3-9, 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 tactile feedback from the device.

Example 3-11. Physical Interaction with an ADVERSE IMPACT on a UFSAR-Described Design Function

Using the same proposed activity described in Example 3-9 and the same UFSAR descriptions from Example 3-10, 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 will be added to the digital design that will emit a clearly audible and distinct "tone" each time the control setting passes through the same setting increment that the tactile feature provided with the mechanical device.

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

of the design function to be performed.

Number and/or Type of Parameters

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.

Potential impacts due to the modification of the number and/or type of parameters monitored should be addressed. The purpose of addressing this aspect is to determine if the number of parameters 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.

Potential causes for an adverse impact on a UFSAR-described design function could include 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 for the operator), the absence of a previously available parameter (i.e., a type of parameter), a difference in how the loss or failure of parameters occurs (e.g., as the result of combining parameters), or an increase in the amount of information that is provided such that the amount of available information has a detrimental impact on the operator's ability to discern a particular plant condition or to perform a specific task.

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 3-12 illustrates the application of the *number and/or type of parameters* aspect.

Example 3-12. Number and Type of Parameters with NO 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.~~

Currently, all controls and indications for a single safety-related pump are analog. There are two redundant channels of indications, either of which can be used to monitor pump performance, but only one control device. For direct monitoring of pump performance, redundant *motor electrical current* indicators exist. For indirect monitoring of pump performance, redundant *discharge pressure* and *flow rate* indicators exist. Furthermore, at the destination of the pump's flow, redundant *temperature* indicators exist to allow indirect monitoring of pump performance to validate proper pump operation by determination of an increasing temperature trend (i.e., indicating insufficient flow) or a stable/decreasing temperature trend (i.e., indicating sufficient flow).

The UFSAR states that the operator will "examine pump performance and utilize redundant plant channels to verify performance" and that the information necessary to perform this task is one parameter directly associated with the pump (motor electrical current) and three parameters indirectly associated with pump performance (discharge pressure, flow rate, response of redundant temperature indications).

A digital system will replace all of the analog controls and indicators. Two control stations will be provided, either of which can be used to control the pump. Each control station will display the information from one of the two redundant channels. The new digital system does not contain features to automatically control the pump, but does contain the ability to monitor each of the performance indications and inform/alert the operator of the need to take action. Therefore, all pump manipulations will still be manually controlled.

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

Commented [D28]: Addresses NRC item 7

Information Presentation

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

The purpose of addressing this aspect is to determine if how the 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.

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

- ~~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 3-13 illustrates the application of the *information presentation* aspect.

Commented [D29]: NEI-initiated to focus on the aspect being illustrated

Example 3-13. Information Presentation with an ADVERSE IMPACT on a UFSAR-Described Design Function

~~Using the pump example introduced in Example 3-12, 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 system 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 on the HSI will be improved to 1 gpm. Furthermore, the HSI will now present the information layout "by channel/train."

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

~~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).~~

With the new display method (i.e., "by channel/train"), additional steps will be required by the operator to determine system performance. The additional steps will require more time, having an adverse impact on the "quickly" design function. Namely, any amount of added time due to the additional actions will increase the total elapsed time and effectively postpone the satisfaction of the "quickly" criterion.

Commented [D30]: Addresses NRC item 7

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.

Operator Response Time

Potential impacts on the overall operator response time should be assessed.

The purpose of assessing this aspect is to determine if the process by which information is obtained is affected by the digital modification in such a manner as to cause 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 relating to operator response time requirements and if those timing requirements are related to the performance and/or satisfaction of a UFSAR-described design function.

For example, the increased time required to perform some control actions (due to the need to call up the appropriate display and operate the "soft" control rather than merely reading an indicator on the Main Control Board) could have an adverse impact on a design function if making and/or implementing a decision based on reading the displayed value is delayed.

Commented [D31]: NEI-initiated addition for completeness

3.2.2.3 COMPREHENSIVE HUMAN-SYSTEM INTERFACE EXAMPLE

Example 3-14. Digital Modification involving Extensive HSI Considerations with NO ADVERSE IMPACTS on a UFSAR-Described Design Function

The purpose of this example is to illustrate the HSI considerations discussed above.

Component controls for a redundant safety-related system are to be replaced with PLCs. The existing HSI for these components is made up of redundant hard-wired switches, indicator lights, and analog meters. The new system consolidates the

information and controls onto two flat panel displays (one per redundant train), each with a touch screen providing "soft" control capability.

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

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

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

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

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

- Consolidation of needed information onto a single display (within the family of available displays) that provides a much more effective view of system operation when it is called into action.
- Elimination of the need for the operator to seek out meter readings or indications, saving time and minimizing errors.
- Integration of cautions and warnings within the displays to help detect and prevent potential errors in operation (e.g., warnings about incorrect system lineups during a test or maintenance activity).

The design was developed using a human factors engineering design, with a verification and validation process consistent with current industry and regulatory standards and guidelines. The design provides a more effective HSI that is less prone to human error than the existing design.

The technical bases for these statements were based on the technical outcomes from NRC-approved and NRC-endorsed sources and using the information considered in those sources to develop those outcomes.

The UFSAR-described design functions applicable to this proposed activity include descriptions of the existing controls, including the physical switches, indicator lights and meters, and how each of these SSCs is used during normal and abnormal

(including accident) operating conditions. The UFSAR also describes how the current physical arrangement (i.e., two physically separate locations) prevents the operator from operating the "wrong" component. There are no descriptions of operator response times associated with using the existing controls.

The impacts on design functions are identified below:

- *Physical Interaction* - NOT ADVERSE because the new HSI consists of two physically separate displays.
- *Number and Type of Parameters* - NOT ADVERSE because the same number and type of parameters exist with the new HSI.
- *Information Presentation* - NOT ADVERSE because all of the existing features (e.g., individual controls, indicator lights and parameters displays that mimic the analog meters) continue to exist with the new HSI.
- *Overall Response Time* - NOT ADVERSE because no response time requirements are described.

Commented [D32]: Addresses NRC item 6