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

INTRODUCTION

Discussion on how Criterion (vi) evaluation compares to the other 10 CFR 50.50 criterion evaluation.

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

Review

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

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

From NEI 96-07, Section 3.9:

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

From NEI 96-07, Section 3.3:

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

Also,

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

Furthermore,

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

Finally,

Commented [MP1]: Note: The yellow highlighted sections are sections that will require changes based on the NRC's comment response to NEI comment on Section C.2.e of RG 1.187 Revision 2.

Commented [MP2]: This review most likely should be altered based on the recommended revisions to steps 5 and 6 in section 4.3.6.

Commented [MP3]: Recommend continuing on with the full paragraph from section 3.3 on NEI 96-07 to discuss the conditions under which intended functions are required to be performed.

> *"As used above, "credited in the safety analyses" means that, if the SSC were not to perform its **design bases function** in the manner described, the assumed initial conditions, mitigative actions or other information in the analyses would no longer be within the range evaluated (i.e., the analysis results would be called into question). The phrase "support or impact design bases functions" refers both to those SSCs needed to support **design bases functions** (cooling, power, environmental control, etc.) and to SSCs whose operation or malfunction could adversely affect the performance of **design bases functions** (for instance, control systems and physical arrangements). Thus, both safety-related and nonsafety-related SSCs may perform design functions."* [***emphasis*** added]

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

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

Commented [MP4]: NEI 97-04, Appendix B Design Basis discussion including Design Bases Functions and Design Basis Values to include discussion of single failures.

1. Design bases functions are credited in the safety analyses.
2. The functions of any individual SSC are functionally below that of design bases functions.
3. Design bases functions are derived primarily from the General Design Criteria.

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

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

Then, from NEI 96-07, Section 3.12:

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

And from the first sentence of the associated discussion:

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

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

Failure Modes and Effects Analysis (FMEA)

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

From NEI 96-07, Section 4.3.6:

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

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

Overall Perspective

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

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

Commented [MP5]: Discussion on Single Failures

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

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

GUIDANCE

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

Determination of "As Likely to Happen As"

From NEI 96-07, Section 4.3.6:

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

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

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

EXAMPLE

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

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

Proposed Activity

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

Qualitative Assessment Outcome

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

Conclusion

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

Determination of Safety Analysis Result Impact

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Commented [MP6]: Add a sentence at the end of this paragraph that discusses descriptive material in the USFAR that does not affect a design function and which can be changed without adversely impacting a design function

For each *design function* identified above, utilize NEI 96-07, Section 3.3 (along with Appendix B to NEI 97-04, as needed) to identify which *design functions* are *design bases functions*, which *design functions* "support or impact" *design bases functions*, and which *design functions* are not involved with *design bases functions*, but are functions that if not performed would initiate a transient or accident that the

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

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

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

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

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

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

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

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

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

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

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

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

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

Step 5: Identify all safety analyses involved.

Considering the scope of design functions and design bases functions from Step 2, identify all safety analyses that rely directly or indirectly on the *design bases functions'* performance/satisfaction. Also, identify all safety analyses related to any other *design function* that could impact either the accident's initiation or the event's initial conditions (i.e., *design functions* that, if not performed, would initiate a transient or accident that the plant is required to withstand).

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

Step 6: For each safety analysis involved, compare the projected/postulated results with the previously evaluated results.

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

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

If any of the identified safety analyses have become invalid due to their basic assumptions no longer being valid, e.g., single failure assumption is not maintained, or if the numerical result(s) of any safety analysis would no longer satisfy the acceptance criteria, i.e., the safety analysis is no longer bounded, then the proposed activity DOES create the possibility for a malfunction of an SSC important to safety with a different result.

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

EXAMPLES

Commented [MP7]: All of the examples will need to be reworked based on the final edits of section 4.3.6.

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

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

Proposed Activity

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

Safety Analysis Result Impact

Step 1:

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

Step 2:

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

Step 3:

Not applicable

Step 4:

Not applicable

Step 5:

The pertinent safety analysis is the accident analysis for Loss of Feedwater. The feedwater control system has a direct impact on the accident analysis assumptions and modeling.

Step 6:

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

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

Conclusion

Although the software CCF likelihood was determined to be **not sufficiently low**, the initiation severity assumed in the Loss of Feedwater accident analysis (four valves affected), the failure mode (valve closure) and the mechanism by which feedwater flow was lost (loss of control signal) remain bounded. Furthermore, the results of the safety analysis, including the type of event (increasing pressure) and all criteria that must be satisfied (maximum allowed peak RCS pressure and maximum allowed secondary pressure) remain bounded.

Thus, the proposed activity does NOT create the possibility for a malfunction of an SSC important to

safety with a different result (for the aspect being illustrated in this example).

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

Proposed Activity

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

Safety Analysis Result Impact Consideration

Step 1:

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

Step 2:

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

Step 3:

Not applicable

Step 4:

Not applicable

Step 5:

The pertinent safety analysis is the accident analysis for Excess Feedwater. The feedwater control system has a direct impact on the accident analysis assumptions and modeling.

Step 6:

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

The minimum acceptable departure from nucleate boiling ratio (DNBR), i.e., the safety analysis result, is 1.30. The current safety analysis result is a minimum DNBR value equal to 1.42. After using the increased value for the new feedwater flow (to represent the increase in feedwater flow caused by the opening of the four feedwater flow control valves) in a revision to the Excess Feedwater accident analysis, the new safety analysis result is a minimum DNBR value equal to 1.33.

Conclusion

Although the software CCF likelihood was determined to be **not sufficiently low** and the severity of the initiating failure has increased, a comparison of the safety analysis results of the minimum DNBR values shows that the new minimum DNBR value remains bounded. Therefore, the proposed activity does NOT

create the possibility for a malfunction of an SSC important to safety with a different result.

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

Proposed Activity

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

Safety Analysis Result Impact

Step 1:

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

Step 2:

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

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

The area radiation monitors perform a function that is necessary to comply with a requirement specified in GDC 64. Therefore, the function of the radiation monitor is a design function directly involved with a design bases function.

Step 3:

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

Step 4:

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

Step 5:

There are no safety analyses that directly or indirectly credit this design bases function. Namely, there are no considerations of malfunctions of single or multiple radiation monitors, or expected responses of the radiation monitors, in any safety analysis.

Step 6:

Not applicable

Conclusion

Although the software CCF likelihood was determined to be **not sufficiently low**, there are no safety analyses that directly or indirectly credit the design basis function or contain expected responses of the radiation monitors. Thus, there cannot be a different result when comparing to a pre-existing safety analysis since none exists.

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

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

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

Proposed Activity

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

As part of the upgrade, each of the chiller's analog control systems will be replaced with a digital control system. Each digital control system maintains all of the operational features (e.g., auto/manual start/stop, setpoints and alarms) as the analog control systems. The hardware platform for each chiller control system is from the same supplier and the software in each chiller control system is exactly the same.

Safety Analysis Result Impact

Step 1:

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

Step 2:

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

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

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

The chiller control system performs a function that supports or impacts the design bases function specified in GDC 20. Therefore, the function of the chiller control system is a design function credited in the safety analysis.

Step 3:

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

Step 4:

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

Step 5:

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

Step 6:

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

Conclusion

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

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

Proposed Activity

Currently, the non-safety-related Steam Bypass Control System (SBCS) and the non-safety-

related pressurizer pressure control system are separate analog control systems.

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

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

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

Safety Analysis Result Impact Consideration

Step 1:

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

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

Step 2:

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

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

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

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

Step 3:

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

Step 4:

If a software CCF occurs, the pressurizer pressure control function, which supports or impacts

the GDC 10 design bases function, will not be performed.

Step 5:

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

Step 6:

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

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

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

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

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

Conclusion

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

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

Example 4-22 illustrates a case in which there is the CREATION of a malfunction with a different result.

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

Proposed Activity

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

Safety Analysis Result Impact Consideration

Step 1:

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

Step 2:

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

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

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

Step 3:

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

Step 4:

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

Step 5:

Numerous safety analyses contain implicit assumptions regarding the performance and/or expectation of the minimum number of system/components and/or trains/channels that are expected to perform their function, which satisfy the applicable redundancy requirements and/or single failure criteria.

Step 6:

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

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

Conclusion

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