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

INTRODUCTION

NOTE: Due to the unique nature of digital modifications, and the inherent complexities therein, the application of this criterion is especially important. Specifically, the unique aspect of concern is the potential for a software common cause failure (SCCF) to create the possibility for a malfunction with a different result. Therefore, rather than simply providing supplemental guidance to that already included in NEI 96-07, Section 4.3.6, more detailed guidance will be provided in this section. However, none of the "more detailed" guidance provided in this section conflicts with that provided in NEI 96-07, Section 4.3.6, or should be construed as being *new*, or *modified* from that in NEI 96-07, Section 4.3.6.

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.

From NEI 96-07, Section 3.9:

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

From NEI 96-07, Section 3.3:

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

Also,

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

Furthermore,

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

Finally,

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

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

A more complete understanding of the meaning of a design basis function 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:

1. Design bases functions are credited in the safety analyses.
2. The functions of any individual SSC are functionally below that of a design basis function.
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 basis 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]

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]

Overall Perspective

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

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

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

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

From NEI 96-07, Section 4.3.6, there are two considerations that need to be assessed when answering this criterion: *credible* and *impact on the safety analysis result*.

GUIDANCE

Determination of Credible

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]

Hence, *credible* malfunctions are defined as those as likely as the malfunctions already assumed in the UFSAR.

If the SCCF likelihood is determined to be **sufficiently low**, then the creation of a possibility for a malfunction with a different result is NOT *credible*.

Alternately, if the SCCF likelihood is determined to be **not sufficiently low**, then the creation of a possibility for a malfunction with a different result is *credible*. If the creation of a possibility for a malfunction with a different result is credible, then further assessment to determine the impact of the malfunction on the safety analysis result must be performed.

Example 4-18 illustrates the NO CREATION of the possibility for a malfunction with a different result due to applying the *credible* consideration.

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

Proposed Activity

A large number of analog transmitters are being replaced with digital transmitters. These transmitters perform a variety functions including controlling the automatic actuation of devices, such as valve stroking, that are credited in a safety analysis.

Conclusion

Based on an engineering evaluation, the likelihood of a SCCF has been determined to be **sufficiently low**.

Therefore, the creation of a possibility for a malfunction with a different result is NOT *credible* and there is no need to determine the impact of the malfunction on the safety analysis result. Without a credible malfunction, the proposed activity does NOT create the possibility for a malfunction of an SSC important to safety with a different result.

Determination of Safety Analysis Result Impact

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.

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 the functions from Step 1. 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.

Utilizing NEI 96-07, Section 3.3, along with Appendix B to NEI 97-04, as needed, 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 no *design basis functions* are involved, proceed to Step 5.

The process for determining if a *design function* is a *design basis function* is aided by identifying the associated General Design Criteria (GDC) to which a *design bases function* applies. Each design function can then be related to the requirements discussed within the GDC to determine if that *design function* is directly involved with the *design basis function* itself or if the *design function* "supports or impacts" the related *design basis function*. If the *design function* is found to directly involve the GDC requirement, then that *design function* is a *design basis function*. If the *design function* "supports or impacts" the GDC requirement, then it is not a *design basis function*, but is still "credited in the safety analysis."

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

If the impact on the *design basis function* involved is readily apparent, no new FMEA needs to be generated, skip this step and go to Step 4. For example, there is no reason to contemplate the generation of a new FMEA if the impact of the SCCF 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 options exist to mitigate potential detrimental impacts on *design functions*.

"Interdependence" is discussed in NEI 96-07, Sections 4.2 and 4.3. 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.

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

If all *design basis 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.

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

Step 5: Identify all safety analyses involved.

Identify all safety analyses that rely directly or indirectly on the *design basis function's* 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 has been no change in the result of a safety analysis and 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, 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 acceptance criteria continue to be satisfied, 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 4-19 through 4-24 illustrate cases in which the SCCF likelihood is determined to be **not sufficiently low** and the creation of a possibility for a malfunction with a different result is *credible*. In these cases, the multi-step process applying the "safety analysis result impact" consideration is performed to determine the impact of the malfunction on the safety analysis result.

Examples 4-19 through 4-23 illustrate some cases of NO CREATION of a malfunction with a different result.

Example 4-19. 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. New components are being added that could fail in ways other than the components in the original design. Now, as a result of this change, all four feedwater flow control valves could simultaneously fail closed following a SCCF.

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 basis function. With no design basis 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:

The severity of the initiating failure for the Loss of Feedwater is unchanged. The event already assumes a total loss of feedwater flow. The newly created failure modes are determined to have no effect on this assumption. The manner in which feedwater flow is lost has no impact on the initial conditions of the event.

Conclusion

Although the SCCF likelihood was determined to be **not sufficiently low** (i.e., the creation of a possibility for a malfunction of an SSC important to safety with a different result is *credible*), the initiation severity of the Loss of Feedwater event, the newly created failure modes and the manner in which feedwater flow was lost do not change the result of the safety analysis. Thus, the proposed activity does NOT create the possibility for a malfunction of an SSC important to safety with a different result.

Example 4-20. 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 SCCF.

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 basis function. With no design basis 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 allowed departure from nucleate boiling ratio (DNBR) to satisfy the accident analysis acceptance limit is 1.30. The current minimum DNBR result is 1.42. After using an 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 minimum DNBR result is 1.33.

Conclusion

Although the SCCF likelihood was determined to be **not sufficiently low** (i.e., the creation of a possibility for a malfunction of an SSC important to safety with a different result is *credible*) and the severity of the initiating failure has increased, the new minimum DNBR result continues to satisfy the accident analysis acceptance limit, which does not change the result of the safety analysis. Therefore, the proposed activity does NOT create the possibility for a malfunction of an SSC important to safety with a different result.

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

Proposed Activity

A complete system upgrade to the area radiation monitors that monitor a variety of containment compartments that could be subject to radioactive releases during a LOCA is proposed. The outdated analog-based radiation monitors are being replaced by digitally-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 Consideration

Step 1:

The functions include the monitoring of the various compartments, rooms and areas that may be subject to an increase in radiation during the recirculation phase of a LOCA.

Step 2:

In this case, whether the function is a design bases function is not readily determined, 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 radiation monitor's function is directly involved with a design basis function.

Step 3:

No new FMEA needs to be generated. The effect of a postulated SCCF on the design basis function involved is readily apparent.

Step 4:

If a SCCF occurs, the area radiation monitors will not perform their design function that supports or impacts a design basis function. Thus, the design basis function will not continue to be performed/satisfied.

Step 5:

There are no safety analyses that directly or indirectly credit this design basis function. That is, there are no considerations of

malfunctions of single or multiple radiation monitors in any safety analysis.

Step 6:

Not applicable

Conclusion

The cited GDC does not contain any reference to single failure protection, so there is no distinction between a failure of a single radiation monitor or multiple radiation monitors.

Although the SCCF likelihood was determined to be **not sufficiently low** (i.e., the creation of a possibility for a malfunction of an SSC important to safety with a different result is *credible*), there are no safety analyses that directly or indirectly credit the design basis function. Thus, there cannot be a "different result" when comparing to a pre-existing safety analysis since none exist.

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 #2, not Criterion #6.

Example 4-22. 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. As part of the upgrade, each analog control system 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 Consideration

Step 1:

The MCRVS also cools the Relay Room that is adjacent to the main control room. The Relay Room contains multiple instrument racks that control both Reactor Protection and Safeguards actuation signals. The air flow path from the Main Control Room to the Relay Room is

described in the UFSAR, along with a function to maintain the Relay Room's temperature less than or equal to 120 ºF.

Step 2:

In this case, whether the function is a design bases function is not readily determined, 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 chillers and the chiller control systems perform a function that supports or impacts the design basis function specified in GDC 20. Therefore, the chillers and the chillers control systems' functions are design functions "credited in the safety analysis."

Step 3:

The impact of a SCCF on the design bases functions 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. Specifically, compliance with existing procedures will direct the recognition of the problem and the restoration of the chiller's function prior to the impairment of the associated design basis functions. In addition, an interdependent procedure change involved the use of the control system "restart" feature to reinitialize the control system, which would clear any software faults, allowing the chiller functions to be restored well before the Relay Room cooling becomes inadequate.

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 Reactor Protection and Safeguards features. As determined in Step 2 above, the chillers' operation 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 basis functions are preserved.

Step 6:

As determined in Step 4, all design basis 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 SCCF likelihood was determined to be **not sufficiently low** (i.e., the creation of a possibility for a malfunction of an SSC important to safety with a different result is *credible*), 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.

Example 4-23. NO CREATION of a Malfunction with a Different Result

Proposed Activity

Currently, the feedwater control system and the pressurizer pressure control system are separate analog control systems.

The feedwater control system is being upgraded from an analog 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 SCCF.

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

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

Safety Analysis Result Impact Consideration

Step 1:

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

Pressurizer - The identified function is control of the pressurizer sprays and heaters.

Step 2:

Feedwater - 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.

Pressurizer - In this case, whether the function is a design bases function is not readily determined, 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 basis function specified in GDC 10. Therefore, the

pressurizer control system's function is a design function and is "credited in the safety analysis."

Step 3:

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

Step 4:

If a SCCF occurs, the pressurizer pressure control function, which supports or impacts the GDC 10 design basis function, will not continue to be performed/satisfied.

Step 5:

The pertinent safety analysis is the accident analysis for Excess Feedwater. Typically, in Chapter 15 accident analyses control system action is considered only if that action results in more severe accident results. The feedwater and pressurizer control systems have a direct impact on the accident analysis assumptions and modeling.

Step 6:

In the Excess Feedwater accident analysis, the initial conditions already assume abnormally low pressure and/or DNBR. Since the pressurizer pressure control system would mitigate the results of the accident, no credit is taken for operation of the pressurizer pressure control system. Therefore, a malfunction of the control system would have no effect on this event and no effect on the safety analysis result.

The severity of the initiating failure is not affected due to the combination of the two control systems. The minimum allowed DNBR to satisfy the accident analysis acceptance limit is 1.30. The current minimum DNBR result is 1.42. After using an 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) and adjusting the appropriate inputs to reflect the new detrimental pressurizer heater and spray conditions in a revision to the Excess Feedwater accident analysis, the new minimum DNBR result is 1.33.

Conclusion

With the SCCF likelihood determined to be **not sufficiently low** (i.e., the creation of a possibility for a malfunction of an SSC important to safety with a different result is *credible*), the severity of the initiating failure has increased. The impairment of the pressurizer pressure control function is

already incorporated in the safety analysis' modeling. The new minimum DNBR result continues to satisfy the accident analysis acceptance limit, which does not change the result of the safety analysis. Therefore, the proposed activity does NOT create the possibility of a malfunction of an SSC important to safety with a different result.

Example 4-24 illustrates a case in which there is the CREATION of a malfunction with a different result.

Example 4-24. 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 the occurrence 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 determined, 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 and are "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 contemplate the generation of a new FMEA since the impact of the SCCF on the design bases functions is readily apparent (i.e., clear and understood).

Step 4:

Performance/satisfaction of the design bases functions related to the GDC 21 and 22 requirements regarding single failure criteria and redundant channels will not continue to be performed/satisfied.

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 simple review of the safety analyses and their structure will quickly identify that the results will exceed the associated acceptance criteria.

Conclusion

With the SCCF likelihood determined to be **not sufficiently low** (i.e., the creation of a possibility for a malfunction of an SSC important to safety with a different result is *credible*), the assumptions regarding redundancy and satisfaction of single failure criteria are invalidated. Therefore, the proposed activity DOES create the possibility of a malfunction of an SSC important to safety with a different result.