The Wording Changes in this Document are for Discussion Purposes only for the September 18, 2019 Public Meeting and have not been Officially Reviewed by all NRC Staff

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

Discussion on how Criterion (vi) evaluation compares to the other 10 CFR 50.59 criterion evaluation (No specific wording provided).

INTRODUCTION

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

Review

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

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

From NEI 96-07, Section 3.9:

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

From NEI 96-07, Section 3.3:

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

Also,

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

Furthermore,

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

Finally,

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

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

A more complete understanding of the meaning of a design bases functions can be obtained by examination of NEI 97-04, Appendix B.

NEI 97-04, Appendix B, states 10 CFR 50.2 design bases consist of the following:

- Design bases functions: 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.

- Design bases values: Values or ranges of values of controlling parameters established as **reference bounds** for design to meet design bases functional requirements. These values may be (1) established by NRC requirement, (2) derived from or confirmed by safety analyses, or (3) chosen by the licensee from an applicable code, standard or guidance document.

This definition of design bases is particularly important for criterion 10 CFR 50.59(c)(2)(vi) because NRC requirements related to **single failures** fall within "Design basis function," as well as, "Design bases values." NEI 96-07, Revision 1, Section 4.3.6, 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." As stated in NEI 97-04, Appendix B, single failures fall within the "Design basis values" because they affect the "values controlling parameters established as reference bounds for design to meet design bases functional requirements." This is captured in the definition of design function in NEI 96-07, Section 3.3, which states, "Design functions are UFSAR-described design bases functions and other SSC functions described in the UFSAR that support or impact design bases functions. 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**." [***emphasis*** added]

The above definition of design basis is also important for 10 CFR 50.59(c)(2)(vi) because it establishes that malfunctions involving single failures are part of the design basis and may be described at any location in the UFSAR, not just in the UFSAR safety analyses. NEI 97-04, Appendix B, states, "10 CFR 50.34(b)(2) requires the FSAR to include a description of structures, systems, and components "…sufficient to permit understanding of the system designs and their relationship to safety evaluations." Thus, design information beyond that considered design bases (i.e., supporting design information) is required to be in the UFSAR. **Importantly**, any malfunction of an SSC important to safety that falls within the definition from NEI 96-07, Section 3.3, of design function, (i.e., which implicitly includes the conditions such as single failure) is part of design basis (rather than part of the description of SSCs required by 10 CFR 50.34(b)(2)) and is required to be considered under criterion 10 CFR 50.59(c)(2)(vi) as a possible "different result."

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 or are required by NRC regulations such as the Emergency Core Cooling System, Station Blackout (SBO) and Anticipated Transient Without Scram (ATWS) rules.
2. 10 CFR 50.2 design bases functional requirements are derived primarily from the principal design criteria for an individual facility (the minimum standards for which are set by 10 CFR Part 50 Appendix A, General Design Criteria) and NRC regulations such as the Emergency Core Cooling System, SBO and ATWS rules that impose functional requirements or limits on plant design. **Importantly**, 10 CFR Part 50 Appendix A, General Design Criteria, defines **single failure** as follows:

   > *Single failure.* A single failure means an occurrence which results in the **loss of capability of a component to perform its intended safety functions**. Multiple failures resulting from a single occurrence are considered to be a single failure. Fluid and electric systems are considered to be designed against an assumed single failure if neither (1) a single failure of any active component (assuming passive components function properly) nor (2) a single failure of a passive component (assuming active components function properly), **results in a loss of the capability of the system to perform its safety functions**. [emphasis added]

3. Design basis functional requirements related to **single failure** is specified in GDC 17, 21, 24, 25, 34, 35, 38, 41, 44, 54, 55, and 56. NEI 97-04 describes, "Examples of Design Bases Controlling Parameters Chosen as Reference Bounds for Single Failure Design," and states "Fluid and electrical systems shall be designed to assure that a single failure, in conjunction with an initiating event, does not result in the loss of the systems ability to perform its intended safety function.

~~1. The functions of any individual SSC are functionally below that of design bases functions.~~

~~2. 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 two sentences, 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. A malfunction that involves an initiator or failure whose effects are not bounded by those explicitly described in the UFSAR is a malfunction with a different result."

Per the definition of single failure, SSCs in which the UFSAR specifies are required to meet single failure, the UFSAR described malfunction/failure is any component failure and UFSAR described effect/result is **no** loss of the capability of the system to perform its safety functions. Specifically, 10 CFR Part 50, Appendix A, General Design Criteria, defines **single failure** as follows:

> *Single failure.* A single failure means an occurrence which results in the **loss of capability of a component to perform its intended safety functions**. Multiple failures resulting from a single occurrence are considered to be a single failure. Fluid and electric systems are considered to be designed against an assumed single failure if neither (1) a single failure of any active component (assuming passive components function properly) nor (2) a single failure of a passive component (assuming active components function properly), **results in a loss of the capability of the system to perform its safety functions**. [**emphasis** added]

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

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

GUIDANCE

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

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.

Determination of ~~Safety Analysis~~Malfunction Result Impact

For cases in which the *qualitative assessment* outcome is a failure likelihood of **not sufficiently low**, the *~~safety analysis~~malfunction 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.* (Note: A UFSAR may include descriptive material that does not affect a design function, which, in effect, 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. 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 malfunctions and results that are explicitly described in the UFSAR and that are affected by the activity~~safety analyses involved~~.

A malfunction that involves an initiator or failure whose effects are not bounded by those **explicitly described** in the UFSAR is a malfunction with a different result. Such malfunctions are not limited to any particular sections of the UFSAR and include, but are not limited to, the accidents and malfunctions described in safety analysis of containment, ECCS and accident analyses typically presented in Chapters 6 and 15 of the UFSAR. Malfunctions and results are related to single failures are considered part of the design basis and therefore, may not be excluded from consideration based on being "supporting design information." The malfunctions and results include those described in the definition of *design function*-which includes ~~This includes~~ explicitly described malfunctions of SSCs and results of postulated single failures and include those described in a FMEA. It also includes UFSAR-described malfunction results described in the definition of *single failure* that fluid and electrical systems are designed to assure that a single failure, in conjunction with an initiating event, does not result in the loss of the system's ability to perform its intended safety function. ~~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 malfunctions ~~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~~malfunction and result the proposed activity could create, ~~involved,~~ compare ~~the projected/postulated results with the previously evaluated results~~ the results with the malfunctions whose results are explicitly described in the UFSAR that are affected by the activity.

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. Comparing the two lists can provide the answer to the criterion question."*
>
> *"A malfunction that involves an initiator or failure whose effects are not bounded by those explicitly described in the UFSAR is a malfunction with a different result."*

Any change that results in a new type of malfunction (i.e., a new mode of malfunction) of a safety system component that leaves that safety system still able to perform it safety functions (e.g., protective actions),

that is, as long as the single failure criteria is not violated, that new mode of malfunctioning of the safety system component should not be treated as a malfunction with a different result.

~~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

{Based on the rewording above, the examples will need to be reworked.}