Draft NEI 96-07, Appendix D

NRC action items from the 9/11/2018 Category 2 public meeting with NEI

1. NRC staff has proposed language below to address the concern with Comment A12.

Comment A12 - Page D8 - Correction (b): Reinsert the below guidance that was deleted from the December 2017 version of Appendix D. This guidance is essential in that it addresses screening of software. Similar wording was also included in RIS 2002-22, Supplement 1.

Proposed language changes to Appendix D Rev 0f text:

An adverse effect may also consist of the potential marginal increase in the likelihood of SSC failure due to the introduction of software. This does not mean that all digital modifications that introduce software will automatically screen-in. For redundant safety systems, this marginal increase in likelihood creates a similar marginal increase in the likelihood of a common failure in the redundant safety systems. On this basis, most digital modifications to redundant safety systems are adverse. However, for some digital modifications, engineering evaluations may show that the digital modification contains design attributes to eliminate consideration of a software common cause failure. In such cases, even when a digital modification involves redundant systems, the digital modification would not be adverse.

Alternately, the use of different software in two or more redundant SSCs is not adverse due to a software common cause failure because there is no mechanism to increase in the likelihood of failure due to the introduction of software.

Reference May 2017 version of Appendix D, ADAMS Accession Number ML17137A020.

2. NRC staff has proposed language below to address the concern with Comment A34.

Comment A34 – Page D21 – This example conflicts with NEI 96-07 by stating that a negative effect on a design function is not adverse and screens out.

Proposed language changes to Appendix D Rev 0f text:

Task 4 is involved. The modification will require the operator to perform four actions in order to manipulate a control (i.e., 1. select the appropriate activity, 2. select the specific component to be controlled, 3. select the control action to be initiated, and 4. execute the action). Currently, the operator is able to manipulate a control in one action (e.g., turn a switch to *on/off*). The HFE evaluation determined that the modification does not negatively impact ~~s.~~ the operator's ability to respond. ~~because the modification increases the difficulty of implementing a response by requiring four actions instead of one action and the additional actions result in an increase in the operator's time to respond.~~

3. Please find attached RIS 2002-22, Supplement 1 that has been highlighted to assist you in resolving comment A40. The staff has highlighted passages to indicate areas of the RIS that should be incorporated in Appendix D in order to resolve the staff's

comments. Although provided in response to comment A40, these highlighted passages may be useful in resolving other NRC comments where RIS incorporation is suggested.

Comment A40 – Page D25 – Proper incorporation of the guidance of Supplement 1 to RIS 2002-22 obviates the need for expansion, refinement or paraphrasing of general 50.59 concepts from the main body of NEI 96-07 revision 1 for evaluation guidance.

4. NRC staff has proposed language below to address the concern with Comment A80. The language provided will resolve A80, however, NEI will need to consider the other NRC comments that have been provided for this subsection of Appendix D. NRC proposed language is not intended to resolve all comments with the subsection.

Comment A80 - Page D48- Correction (a): This is an open issue documented in the meeting summary from the 11/30/2017 public meeting (ML17331A485), which states:

The NRC staff pointed out that Title 10 to the Code of Federal Regulations (10 CFR), Section 50.59, (10 CFR 50.59) "Changes, test and experiments," used the term "final safety analysis report (as updated)" while NEI 96-07, Appendix D, Section 4.3.6 used the terms "safety analysis" and "accident analysis." The NRC staff said that it could be understood that "accident analysis" is a subset of "safety analysis" which is a subset of "final safety analysis report (as updated)." Using more restrictive terms, it could be understood that the evaluation guidance only addressed a subset of "any [malfunction] previously evaluated in the final safety analysis report (as updated)."

Proposed language changes to Appendix D Rev 0f text:

> Determination of Malfunction ~~Safety Analysis~~ Result Impact
>
> The generic process to determine the impact of a malfunction of an SSC important to safety on the results on SSC malfunctions previously evaluated in the UFSAR~~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.
>
> Moreover, in cases in which an activity involves a component that is not described in the UFSAR, the effect of the component on the system of which it is a part needs to be considered. Likewise, the impact of an activity involving a non-UFSAR subcomponent on equipment that the subcomponent supports needs to be considered.
>
> In addition, 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 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." As described in NEI 96-07, Section 4.3.2, the safety analysis assumes certain design functions of SSCs in demonstrating the adequacy of design. This process should include both direct and indirect effects on the design functions.

The safety analyses will not usually list all of the components that are relied upon to perform design functions. Therefore, the review should not be limited to components discussed in the safety analyses. For example, performing a design change to a controller for valve in the high pressure safety injection system would be considered to involve SSC credited in safety analyses even though the valve itself may not be mentioned in the safety analyses.

Step 5: Staff's recommendation of this step was provided in response to action item #5, below.

Step 6: ~~For each safety analysis involved, c~~Compare the projected/postulated results with the previously evaluated results~~.~~ to determine whether the effects are explicitly bounded by the results in the USFAR.

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."*~~

5. NRC staff has proposed language below to address the concern with Comment A85. The language provided will resolve A85 in its entirety (parts a, b, and c as labeled by NEI).

Comment A85 – Page D50 - **Correction (a):**
Questions (vi) is meant to address "new' or different malfunctions; there will never be any "pre-existing safety analysis" for new types of malfunctions created by a change. Based upon the reasoning stated here, it could potentially be understood that malfunctions such as CCF would not be considered a different result if not previously analyzed. This would be contrary to Questions (vi) under 50.59.

Proposed language changes to Appendix D Rev 0f text:

Step 5: Identify malfunctions previously evaluated in the UFSAR and the results of these malfunctions.

Identify any malfunctions of SSCs important to safety previously evaluated in the UFSAR for the SSCs affected by the activity. Importantly, 10 CFR 50.59(c)(2)(vi) explicitly requires the comparison as a "different result than **any** previously evaluated in the final safety analysis report (as updated)." Therefore, criterion 10 CFR 50.59(c)(2)(vi) requires malfunctions evaluations located throughout the UFSAR to be considered. This includes malfunctions evaluated in supporting UFSAR analyses of individual SSCs (e.g., failure modes and effects analyses) that analysis demonstrate that SSC design functions will be accomplished under required conditions, such as equipment response times, process conditions, equipment qualification and **single failure**. Other malfunctions previously evaluated that are required to be considered include, but are not limited to malfunctions discussed in safety analyses (e.g., containment, ECCS and accident analyses typically presented in Chapters 6 and 15 of the UFSAR).

While accidents are discussed primarily in the accident safety analysis typically presented in Chapter 15 of the UFSAR, discussions of other malfunctions are scattered throughout the UFSAR in various places (e.g., the FMEA or single failure consideration previously evaluated in UFSAR chapters of individual SSC). To address this criterion, it is important to locate each discussion of a malfunction in the UFSAR and evaluate the description and implication about the effect of the failure.

NOTE: Not all design functions are credited in the safety analysis. Some design functions are required for other reasons (e.g., to meet regulations or to eliminate malfunctions and accidents.)

~~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.~~

~~7.~~6. NRC staff recommends either deleting this example, as it does not belong under section 4.3.6, or moving the example to section 4.3.2 or 4.3.5 of Appendix D. As written, this example does not provide any guidance or insight into Criterion 6.

Comment A87 – Page D55, Example 4-21- This example points one of the concerns with the reasoning embodied in the multi-step process. One of the ideas is that a change should not more than minimally impact the "consequences" which in 50.59 means dose. "Consequences" is a subset of "results". The radiation monitors are used, in part, to limit dose, so a misbehavior in that system could adversely impact dose.

Question (vi) is meant to address "new' or different malfunctions; there will never be any "pre-existing safety analysis" for new types of malfunctions created by a change.

~~8.~~7. NRC staff will withdraw A89 as comment under Example 4-23. There is no action required by NEI for this comment.

Comment A89 – Page D58 - Example 4-23 - Staff does not believe that this step (step 4) is representative the level of complexity of mods that are being conducted in the field. NEI requesting NRC to suggest a more complex example.

~~9.~~8. On Page D47, the staff notes that the referenced 63 FR 56106 is a proposed rule and not the final rule. NEI should reference final rules in its guidance, as there are differences between the proposed rule and final rule.